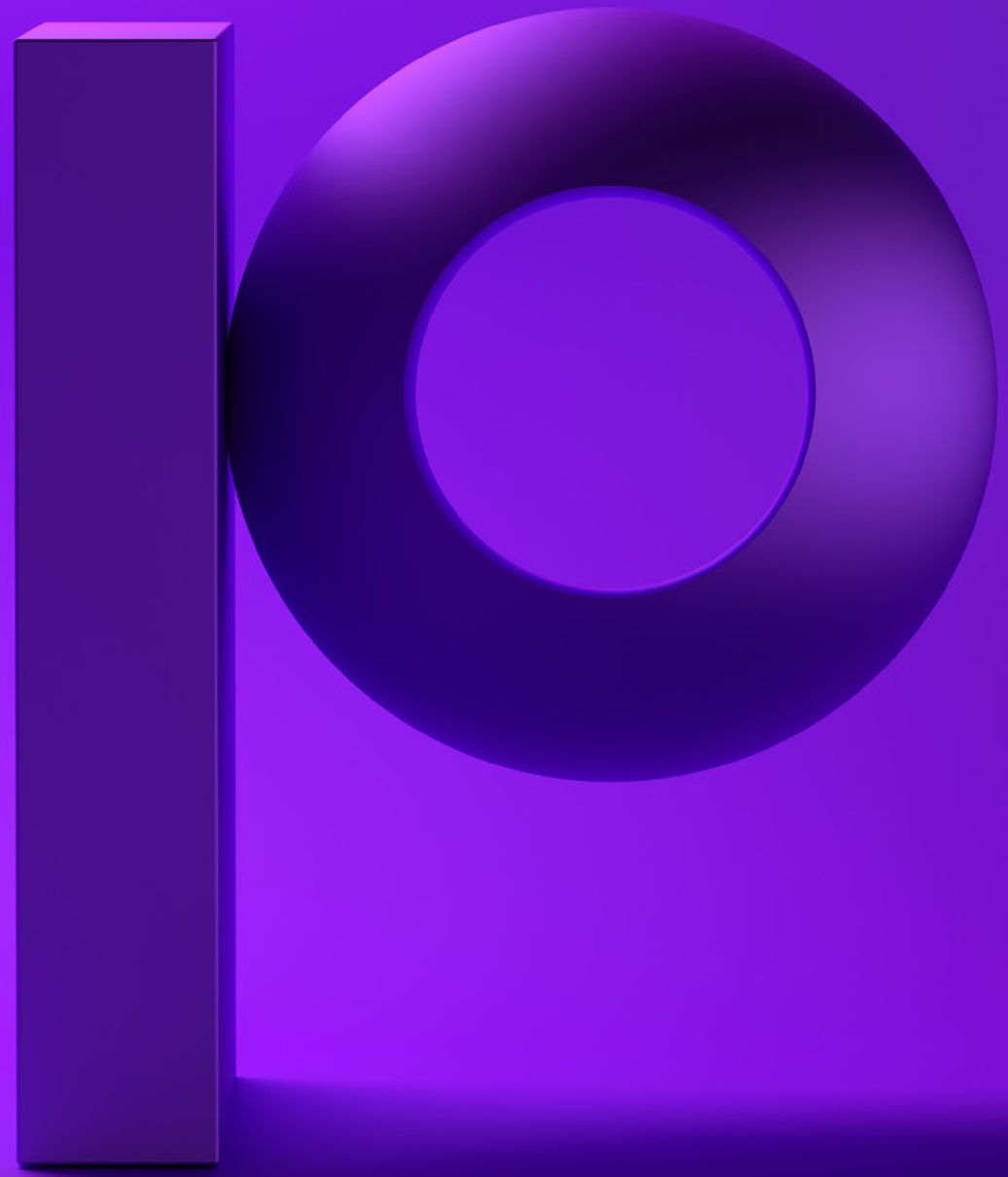
precisely

# How malware is reshaping IBM i security

## The rules have changed



# The futility of incremental security upgrades

No matter what business you are in, and no matter your department, your role, or your level of responsibility within it, the unending reports of data breaches and ransomware attacks have probably resulted in an equally unending string of long, sometimes overwhelmingly technical IT security meetings and training sessions. It can seem as though we all need to become cyber security experts, just to keep our day jobs.

Sadly, that sentiment is not far from the truth.

Even for technical professionals like networking engineers, database analysts, application developers and web marketing managers, IT Security has traditionally been viewed as something of a 'back office' function, with specialist wonks working tirelessly to protect the business from phishing attacks and hackers hunting for social security numbers. "They do their job, so I can focus on doing mine." But this way of working has simply become too risky.

And this is not only because of the exponential increase in frequency and scale of cyber attacks. The real problem is that the very nature of cyber threats has changed radically. Countering them requires a business-wide shift to informed, cooperative and inclusive IT security planning management practices. To get the buy-in and cooperation to make this shift happen requires that executives and business leaders in every department understand how today's advanced threats actually work and just how lethal they can be to the business.

In this eBook you will find practical and shareable explanations of malware and ransomware attacks; the core security technologies and methods available for dealing with them; and perspectives on how to apply and align those technologies and methods for maximum defensive value.

# The rise of the cyber-insecurity industry

The first thing we all need to understand and accept is that malware and ransomware are a very profitable range of cyber-attack products and services which are marketed and sold by a wide range of 'companies,' large and small, who make their living in the Cyber Insecurity industry.

If that seems like a bit of an exaggeration, it is not. In fact, it is exactly the steady, organized industrialization of cyber attack tools and services over time which has led to what seems like a very sudden outbreak of advance cybercrime. The malicious software and attack methods we are now seeing are just the latest products coming from a well-developed and growing 'Third-Party Developer Community' operating within a lucrative global marketplace.

Their offerings include a wide array of highly engineered proprietary tools and open source commodity products, as well as a rapidly-growing Ransomware as a Service sector.  In addition, just as with any other developer community, skills development and transfer are continuous and highly crowd-sourced, which of course means more rapid advancements in features and process efficiencies.

And, of course, all these product and service development efforts are funded and fueled by a very efficient 'Dark Web' marketplace for the sale and resale of the data and industrial intelligence gained by using those products and services.

The bottom line is that you are not up against a few, exceptionally clever and evil bad actors. The cyber criminals are highly organized and well-funded, and are rapidly becoming a major threat to the global economy... and to your organization.

## The fundamental architecture of next-gen cyber threats

After so many years of development, testing and refinement, the core features and methods included in state-of-the-art malware and ransomware attacks have now begun to coalesce around four basic characteristics:

- **Actively guided**
  No longer are you just dealing with toxic chunks of malicious code that are downloaded or triggered upon invite, or that execute a single, standardized sequence of actions. Increasingly, malware is actively guided and executed by a skilled and knowledgeable hacker who has gained access to your systems.

- **Stealthy / nearly invisible**
  Attack execution does not rely upon artificial intelligence. It is real human intelligence that is analyzing the situation, evaluating targets, considering tactics, and figuring out how to overcome unexpected obstacles. Skilled, responsive, resilient. Because there is a real human being in control, it can be nearly impossible to distinguish the hacker's activities from 'normal' user or application activity.

- **Driven by monetary gain:**
  The latest generation of cyber-attack tools and methods have proven repeatedly that they work reliably, and given the potential profits involved, a rapidly growing number of hackers world-wide are willing to invest heavily in the IT skills development, computing and network resources and labor time required to be successful.

- **Crypto Currency-Enabled:**
  Finally, the rise of crypto currencies and their very private and very liquid global trading systems have made them the "Unmarked Bills" demanded for all 21st century cyber extortion. Essentially untraceable and so easily traded and/or converted to normal currencies, crypto currency movements are effectively completely unregulated and nearly untraceable by law enforcement agencies and modern global financial controls.

The key point here is that in order to realign your organization's security stance to one which more fully guards against modern malware threats, it is vital to get executives and team members all across the company to break old habits and to change outdated attitudes and beliefs about IT security. Having a more accurate and practical understanding of today's threats will go a long way toward convincing them to pay attention and cooperate with your organization's the new IT security rules and processes.

# Focus on defense, not prevention

Human-guided IT breaches and subsequent discovery and execution activities are by definition completely variable. Thus, there is no way to develop and deploy standardized profiles or signatures by which they can be automatically identified. Traditional automated scanning, alerting and remediation practices are also no longer enough. Increasing Hands On or Ad Hoc systems surveillance is also a losing battle plan. In the end, completely and reliably preventing malware and ransomware attacks is just fundamentally impossible.

Instead, your IT 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 creativity. This, in turn, demands that your focus needs to be upon securing critical assets and data stores using a multi-layered defensive approach.

This is not to say that your existing IT security tools and systems are obsolete or no longer effective.  Rather, it means applying them in an overall context of sequential, layered defenses, employing every security option you have available, but in a coordinated, programmatic way.

Minimum requirements include:

- Automated, integrated security monitoring and alerting
- Multi-Factor Authentication (MFA)
- Zero Trust and Least Privilege Authority
- Aggressive use of VPNs
- Pervasive Data Encryption / Tokenization
- Frequent and encrypted offline DR backups
- Logical and Physical network segmentation and control
- Continuous security analysis and reporting

## Agile defense requires active communication

In addition to thinking more defensively about how you apply security tools and systems, it is just as important to focus on establishing highly coordinated, cooperative, and responsive processes for dealing with potential and actual security incidents. The maxim "See Something, Say Something" is a good standard when defending against malware and ransomware attack.

This is not to say that every anomaly generates a full cyber attack alert. Rather, the goal is to assume a truly defensive stance, responding in a more wholistic manner by maintaining continuously open and active team communications, or what you might call a system of focused, purposeful "chatter" between web ops, network management, database management, etc.  This enables earlier, faster, and more focused assessment and response.

For example, if one team member notices some seemingly minor yet unusual activity on, say, a web commerce server, they should not only check it out, but also advise other IT leaders and functions about it. That web commerce server anomaly may be quickly explainable by the app development team (and maybe added to their running bug list). Or it may raise a red flag with a database manager who has recently seen a few instances of corrupted data in a related database table.

The most important point is this: Focus on defense, maintain continuous communication, and train everyone for agile, coordinated response to any potential cyber attacks.

## The threat to IBM i systems

IBM has always built comprehensive advanced security capabilities into IBM i, giving the platform a sterling reputation for system security and data protection. But even IBM itself says that IBM i servers are highly securable, not inherently secure. They still require careful and focused management to ensure that all the appropriate security options are properly implemented.

In addition, there is no doubt that IBM i hardware, applications and data are increasingly integrating with other platforms, across your enterprise and across the web to partners, service providers and cloud-based e-commerce systems. Which means that although your IBM i servers may not be where the malware mastermind first gets into your systems, any gap in your IBM i security configuration could mean the hacker gets a peek at some useful bit of information such as a standard default password for new user profiles.

Armed with that tiny clue, the hacker may then programmatically prowl around for weeks, watching for a new user profile to be created so that he can "register" himself before the intended new user does so.

And finally, given the highly competitive, bitcoin-fueled continuous development programs that are active across the Cyber Insecurity industry, assuming that IBM i is so secure that there is no incentive for hackers to figure it out is an increasingly risky stance. Put another way, if you can attend advanced IBM i security training classes, so can they.

# Building a multi-layered defense

**Defending against breach – external and internal points of entry**
The first layer of defense against malware and ransomware involves establishing and enforcing strict security protocols that ensure effective, automated control over every point and method of access. This must include controlling access from external sources, of course, but it is just as critical to defend against insider threats because cyber-thieves prowling your systems have become so expert at blending in with your employees, contractors, and business partners, and even your security team.

A central feature of IBM i security is the granting and control of special or "elevated" access authority to users, on an individual basis or by assigning them to a group-specific user profile. Some roles have a valid business case for having access to data such as customer lists, source code, financial information, intellectual property, employee HR files, and other information. But too often, less than strict control over access rights results in too many overly powerful users, or temporary permissions that are never actually revoked, resulting in multiple easily exploited options for a ransomware attacker to leverage.

Compounding this problem is excessive reliance upon basic password-based authentication and single sign-on. The many weaknesses of passwords as security are legend. But at root, they are weak because they are so simple to use, and just as easy to share or lose. It only takes one errant sticky note to open up your entire organization to a devastating ransomware attack.

The IBM i platform includes extensive options for applying access controls, not just for logging in but for limiting or denying access to systems and data on a very granular level. However, manually establishing and maintaining effective and detailed access controls can quickly become overwhelming even for smaller organizations and does not scale easily for managing large and complex environments.

So, to enable and maintain security against breach, it is necessary to fully apply state-of-the-art security technologies such as those discussed earlier.

## Hardening the ultimate targets – data at rest and in motion

With rare exception, the primary motivator for cyber-criminals is financial gain. And they understand that your data is your most precious asset. So, all their techno-trickery is ultimately directed at finding and "kidnapping" your data via encrypting it. Experts talk about remediation after a breach, focusing on recovering data and repairing systems. But after a fully successful ransomware attack, with your data locked up by unbreakable encryption, remediation is incredibly difficult, time consuming and very, very expensive. In some cases, it may be completely impossible.

To help ensure that the situation never gets to that point, it is critically important to make your data a "hard target" both by making it much harder to find and rendering it essentially worthless to hackers by encrypting it before they can get to it. This fundamental requirement applies to all your data, wherever it exists, and at all times.  It applies while data is being viewed, created, or modified in a production system; while it is being used in development testing; or as it is being sent and received across internal or external network connections.

And, for complete defense against malware and ransomware attacks, all HA and DR backup data must also be encrypted and maintained in storage systems which are beyond the reach of cyber-criminals.

## Monitoring for signs of compromised security

Effective multi-level security defense can only be achieved if, for each layer and method of security implemented, the assumption is made that it will eventually be defeated. This means a mindset that repeatedly asks what happens next, not if but when any given layer of defense fails. In the case of advanced ransomware threats, it must be assumed that cyber thieves will get in. At that point, your security strategy must shift from preventing breach to detecting it.

Because of the advanced human-operated, intelligent user-spoofing tools and methods employed by cyber-crooks, this is no simple matter. It becomes an almost fuzzy-logic process to surveil systems and identify seemingly normal events that, considered in isolation, may not be enough to warrant investigation but which may in fact indicate an attack may already be in progress.

This is especially difficult when the attacker is careful to make only tiny, incremental moves or changes and to limit total activity to short, non-obvious frequency or elapsed time. This "burrowing" phase, during which the attacker remains quiet most of the time, can go on for days and weeks, or even months while elevated privileges are acquired and additional accounts, systems and data sets are compromised.

Defending against malware and ransomware in this phase requires deep, granular and automated monitoring along with a comprehensive, enterprise-wide view to analysis, alerting and reporting. A very small yet odd event on your IBM i platform, such as downloading just a few records under a privileged vendor's profile, can indicate big trouble for your entire enterprise if, in fact, that vendor is no longer active in your payables systems or has not logged in for several months.

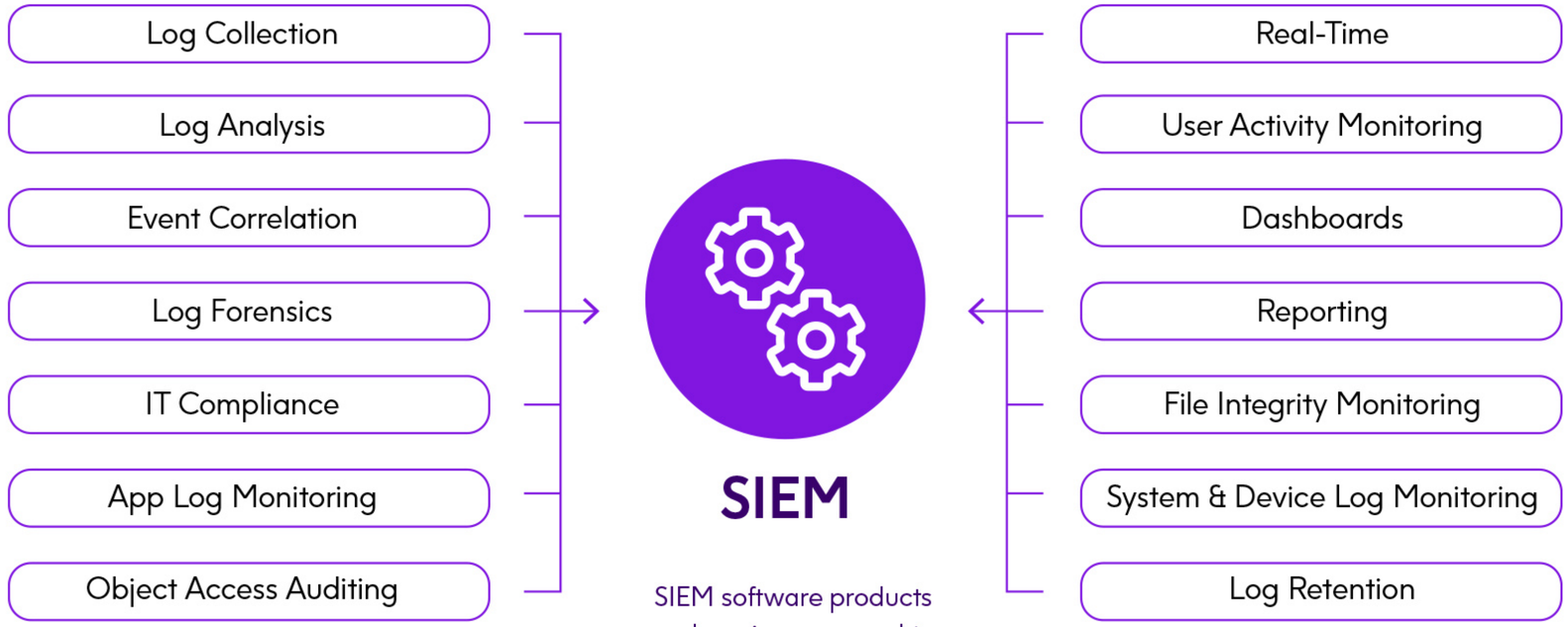
Only through truly automated and integrated, cross-platform security monitoring and analysis, combined with vigilant team members that truly communicate with each other, can such tenuous logical connections become an actionable indicator of compromise (IOC).

## Integrating and coordinating security systems and processes

Ultimately, the strongest and most effective security is only achieved through rigorous contingency planning and the coordination of multiple security elements to surround the target with multiple layers of defense.

Security Information and Event Management (SIEM) solutions are integral to security strategies for many organizations today. Because IBM i is deeply integrated operationally with all your other systems and platforms, it is critical that IBM i security is also as fully integrated into your overall security plans and systems as possible.

Due to the wide range of security log sources which need to be integrated, as well as the proprietary nature of its data formats, integrating IBM i security information into an enterprise SIEM platform through in-house development and maintenance can be challenging and time consuming, requiring specialized, platform-specific skills. The key is to implement a third-party solution to automate the monitoring and presentation of IBM i security log data to your SIEM solution.



# Reboot required to apply changes

In a way, this focus on integrating and coordinating all elements of your security systems and processes leads us right back to the beginning of this eBook. None of the perspectives and recommendations offered here can be applied with any real hope of success unless everyone in your organization has a realistic view of the nature and severity of today's advanced threats and is willing (and empowered!) to actively participate in defending against them.

But first they will need help to get past their existing frustration with continuously escalating IT Security directives. As always, the most effective tool is to help everyone understand the "Why?" behind the rules and processes the organization is putting in place. Supportive and role-appropriate explanations of the preceding concepts and recommendations will go a long way toward reaching that goal.

By the same token, broad discussions of strategic approaches to defending against malware and ransomware are clearly not enough to enable implementation. Nor can a single eBook provide a sufficiently detailed assessment of the tools, systems and processes you will need to move forward with building your defenses.

To help you get started, here are some links to key resources and leading organizations who can help you go deeper into the details of core requirements and best practices for building up your malware defenses:

**UK National cyber security centre:**
Mitigating malware and ransomware attacks

**U.S. NIST Cyber security resource center:**
NISTIR 8374 - Cybersecurity framework profile for ransomware risk management

**U.S. Cybersecurity & infrastructure security agency (CISA):**
MS-ISAC ransomware guide

**IBM Security™ X-Force® threat intelligence research hub:**
The definitive guide to ransomware: Readiness, response, and remediation

# Precisely can help

Building more effective defenses against malware and ransomware starts with a thorough evaluation of your current security stance and future requirements, led by by your security administrator, compliance team, and management. It also helps to bring in outside experts who understand the available technology options and can help focus and accelerate your evaluation.

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, Precisely is here to help you enhance your IBM i security.

### Precisely Security Software for IBM i

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

- Control of network access, database access, and command access
- 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

### Precisely 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 by:

- Performing 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.
- Providing 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.
- Assisting your team during compliance or security audits by generating reports required by your auditors.
- Ensuring a successful implementation of Precisely security technologies and providing all needed training.

precisely

Precisely is the global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 97 of the Fortune 100. Precisely's data integration, data quality, data governance, location intelligence, and data enrichment products power better business decisions to create better outcomes. Learn more at www.precisely.com.

**www.precisely.com**