Staying safe from ransomware with IBM z Systems

Keep mainframe data safe from malicious encryption with a comprehensive, strategic approach
The growing threat of ransomware to enterprise data

The threat of ransomware strikes fear in organizations—from small businesses to large enterprises. Ransomware has been in the headlines many times and continues to be a top concern. Hospitals, educational institutions, financial services, utilities and even the San Francisco MTA have been breached.

Ransomware is malware that is designed to lock up an endpoint—whether that’s a personal computer, a mobile device or a server—by revoking access to the device, or by encrypting the data it contains. To sneak the ransomware onto a system or network, cybercriminals may use social engineering to entice users to open malicious attachments, or hack in through a privileged user’s compromised account. Typically, once the malware is activated and data is encrypted, a ransom screen appears with instructions for how to pay for the decryption key. Although law enforcement agencies advise against paying the ransom, many businesses give in: They cannot afford to lose their data.

Some noteworthy statistics on the prevalence of ransomware attacks:

• IBM® X-Force® has seen an increase in ransomware attachments to spam, up from an average ransomware attachment rate of 0.6 percent in 2015 to nearly 40 percent in 2016.¹
• While on-screen ransom requests average about USD500,¹ businesses are experiencing larger-scale ransomware attacks, with demands ranging from thousands of US dollars up to millions of US dollars in nearly untraceable cyber-currency.
• According to US government statistics, ransomware incidents quadrupled in 2016, with an average of 4,000 attacks a day.¹
• According to X-Force, ransomware continues to be one of the most profitable forms of malware in terms of effort versus earnings.²

Learn more from IBM X-Force about ransomware threats.

Mainframe advantages

A vast share of essential corporate information originates or resides on mainframes to take advantage of their reliability, security, availability and reduced cost. Fortunately mainframes are inherently much more secure than workstations and mobile devices. Some advantages available in the mainframe include:

- Integrated security across IBM z Systems® processor, hypervisor, operating system, communications, storage, database and application software
- Data-security features including pervasive encryption implemented at all levels from storage to database and application controls
- Integrated security support for the extended enterprise among z Systems and IBM Security solutions
- z Systems software supporting compliance with government and industry regulations including the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), the European Union's General Data Protection Regulation (GDPR), Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) and others
- An extensive portfolio of security certifications for z Systems hardware and software including Common Criteria at EAL5+ and FIPS 140

Nonetheless, if the system account of a privileged user such as a database administrator is compromised, malware can be introduced into the system. Even the most secure mainframe can be vulnerable to privileged user threats, if these entitled users are not adequately protected with strong authentication, access controls and segregation of duties to reduce the potential exposure. Vigilant logging and auditing help in watching over privileged users and mission-critical information. And if all else fails, the mainframe has outstanding capabilities for backup and recovery of applications and data.

Learn more about z Systems security.

Ransomware-mitigating mainframe capabilities

There are several technical capabilities mainframe administrators can employ to help deflect ransomware attacks, including:

- **Strong authentication:** Two-factor authentication solutions such as IBM Multi-Factor Authentication for z/OS® with RSA SecurID token or IBM TouchToken (supporting one-time passwords) can protect privileged user credentials. Alternative authentication such as passphrases and biometrics are also helpful.

- **Timed login window:** A privileged identity policy can mandate that privileged users such as the IBM DB2® admin ID are temporarily issued based on change control ticket. Accounts can also use an IBM Security Privileged Identity Manager "library card" to sign on to privileged user IDs.

- **Data activity monitors:** Another best practice is to utilize a database activity monitoring solution such as IBM Security Guardium®. With Guardium, policies can be created to monitor database activity and react to unusual traffic.

- **Performance monitoring:** An attack could also be discovered based on the data encryption overhead statistics in IBM System Management Facility (SMF) data. Mainframe platform monitoring solutions such as IBM OMEGAMON® can be used to detect and pinpoint the rogue code.

- **SIEMs and auditing:** Security solutions can also help detect and mitigate threats. IBM Security zSecure™ Alert can notify operations or security teams that a suspicious activity is in progress. IBM Security zSecure Audit collects, augments and reports on all security-related events on the platform showing suspicious activity. zSecure Alert and zSecure Audit can send real-time security events to a centralized security information and event manager (SIEM) such as IBM QRadar®, which can correlate mainframe events with other events in the enterprise to identify the initial entry point of the attack. User-behavioral analytics running within QRadar can proactively identify insider threats based on changes in user behavior.

- **IBM Secure Service Container:** The container provides industry leading isolation from peers, vertical isolation and protection of data from privileged administrators. It also provides automatic encryption of data and code (at rest and in flight) and validation of application code to help reduce the risk of tampering or malware.

60% of all security attacks in 2015 were by insiders.

Learn more about protecting privileged users.

IBM Security solutions for mainframe protection

The superior security found on today’s mainframes helps deter ransomware threats. IBM provides a number of security solutions and services to help organizations defend against these threats, including:

- **IBM Resource Access Control Facility (IBM RACF®):** Identifying and verifying system users, administering privileges, and authorizing users’ resource access
- **IBM Multi-Factor Authentication for z/OS:** Enforcing strong multi-factor authentication with RSA SecurID tokens and IBM TouchToken
- **IBM Security Identity Governance and Intelligence:** Delivering detailed analysis of roles and entitlements to align with business processes and rules to prevent over-entitlement
- **IBM Security Privileged Identity Manager:** Helping prevent insider threats by securing and auditing privileged identities
- **IBM Security Guardium:** Identifying sensitive information, controlling database administrators and monitoring their activity
- **IBM Guardium Data Encryption:** Encrypting and protecting critical information assets
- **IBM QRadar SIEM:** Consolidating enterprise log events, analyzing threats, providing real-time visibility and prioritizing alerts
- **IBM Security zSecure Adapters for QRadar SIEM:** Collecting and integrating real-time mainframe security events, replacing manual analysis with automated detection
- **IBM Security zSecure Admin including the Admin Access Monitor:** Automating RACF tasks to manage identities and identifying unused access privileges to prevent vulnerabilities
- **IBM Security zSecure Alert:** Providing predefined alerts for common conditions and customizable alerts for business needs
- **IBM Security zSecure Audit:** Gathering and analyzing critical information and delivering customized reports on threats
- **IBM Security zSecure Command Verifier:** Finding and blocking noncompliant RACF commands before execution

Learn more about how to outthink threats on the mainframe.

---

Recommended best practices for avoiding ransomware

Utilize these general security best practices along with IBM Security solutions to help avoid potential ransomware threats:

- Educate users to raise awareness of phishing, spamming, suspicious attachments and other threats
- Utilize appropriate security solutions to detect malware in email, communication and browsers
- Minimize privileged-user entitlements to ensure least possible privilege and segregation of duties
- Require privileged users to use strong multi-factor authentication such as one-time smart tokens and biometrics, especially on mobile devices
- Clean up your security database regularly to remove any obsolete, old or unnecessary security permissions, especially for terminated employees
- Audit all security-relevant security events, especially privileged user actions and sensitive data access
- Monitor security status and events with real-time analytics that help detect and prioritize threats and issue alerts
- Encrypt and access-protect all sensitive, proprietary and personally identifiable (privacy) information
- Create backup copies of all essential information frequently and protect that information accordingly with encryption and access controls
- Document the disaster-recovery process to restore your data; practice these processes with recovery drills
- Stay current on operating system, database and security patches and updates to minimize known exposures
- Always remember that enterprise security is only as strong as your weakest link

Learn more about best practices for mainframe security.

Utilize comprehensive security solutions from IBM

Mainframes are an important part of your business enterprise, housing mission-critical corporate information. The mainframe is one of the most secure platforms for business applications that require 24x7 availability of business information. z Systems feature native security advantages such as RACF and hardware cryptography, but they can also take advantage of the extensive portfolio of IBM Security solutions, providing an intelligent, multi-layered immune system to effectively thwart ransomware and other threats.

Learn more about the full portfolio of IBM Security solutions.
Why IBM?

With the volumes and value of data and mission-critical applications that mainframe systems hold, they are a valuable target for cyber attacks, including potentially devastating ransomware attacks. Because mainframes are very often the system of record for the most valuable data that an organization possesses, ransomware can be particularly damaging.

The best barrier to ransomware is to deploy comprehensive security tools and practices that can detect and block attacks on several fronts, not just the mainframe itself, with a mix of analytics, reporting and proactive security remediation. Together, these tools — such as RACF, zSecure Admin and zSecure Audit, IBM Security Identity Governance and Intelligence and Guardium — can act as an electronic immune system to provide a comprehensive, integrated security model. These tools, guided by intelligent access policies, can help you protect your mainframe by allowing access only to the right people, and only for the purposes that make sense in your business context.

Other tools, such as IBM QRadar SIEM and IBM Resilient Incident Response Platform Enterprise help round out the security environment in which your mainframe and its valuable data reside, by giving enterprise-wide security visibility to system administrators.

IBM delivers deep knowledge, expertise and experience in mainframe and identity and access management, as well as in other aspects of network and data security. With IBM, you can achieve mature identity and access governance with integrated solutions designed to meet mainframe needs and security threats in your modern enterprise.

Learn more on the web about IBM Security.
For more information

To learn more about IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security solutions
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing