Outthink threats with analytics and security intelligence for IBM z Systems

Address the big security picture with integrated capabilities for mainframes and the security operations center
To avoid security risks, address the entire environment

When it comes to enterprise security, you can’t afford gaps. You can’t afford silos. In fact, you can’t afford anything that prevents full visibility into and strong control over what’s happening on your network, systems and applications. Today’s business demands are simply too high—and the risks of incomplete security are simply too great.

Can you afford to lose USD4 million? That’s the worldwide average cost of a data breach today.1 How about EUR20 million (about USD22 million) or 4 percent of your total worldwide annual turnover? That’s the potential sanction for noncompliance with the new European Union General Data Protection Regulations (GDPR).2

Yet many organizations take precisely these risks. It’s not that they intend to. Often, it’s simply that they’re not doing all they can do—and not seeing all they can see—to understand and control network, systems and application activity in complex environments. This can be especially true for environments that include both mainframe and diverse technologies.

For more than 50 years, IBM mainframes have been industry leaders in providing a secure base for critical business operations—right up to today’s IBM® z Systems®. Security capabilities are built into the entire z Systems stack. But today, the responsibility for monitoring, assessing and defending the overall enterprise—with its high use of less-securable systems, from desktops to laptops, tablets and mobile phones—resides with the analysts in the security operations center (SOC). In today’s high-demand, high-performance, high-risk business and computing environments, what enterprises need is a new way for mainframe and SOC administrators and technologies to work together.

Learn more from IBM X-Force® about current threats.

---

Use tools from the SOC to improve mainframe security

Due to their long history in the data center, the business-critical data that typically resides on them, and the specialized skills necessary to administer them, mainframes have long been managed in silos. They have stood apart from the diverse, end-user operated systems that populate much of the enterprise. But threats to system and data security are on the rise everywhere. One recent study predicted a 25.6 percent likelihood that any given enterprise would lose more than 10,000 records to a data breach by 2018.1 Mainframes are not immune. In fact, while many security initiatives focus on less-securable devices, applications and data, the increased awareness of cyber threats has also exposed potential vulnerabilities in mainframes. These threats can include system-wide shortcomings (security features that are not properly activated) that open the entire enterprise to breaches; specific vulnerabilities (lack of controls over data access by privileged users) that invite insider theft; and lax practices (inability to monitor and report on system activity) that can result in noncompliance with regulatory standards.

Meanwhile, in the SOC, analysts facing many of the same issues for diverse systems employ proven tools to improve security including: constant monitoring at the device, application and user levels; identity governance and administration; deep analytics; automated intelligence; and comprehensive auditing and reporting.

Now you can include your mainframe environment in this same security management framework, enabling big-picture visibility into your entire security landscape, timely actions for building defenses before an attack and responding in real time when an attack occurs, and integrated management of your enterprise security activities.

---

The big picture: Get the visibility and intelligence you need

A siloed system lives in its own world—one that’s not only separate but is often used to house sensitive data warehouses that require high levels of security. It’s a world where large mainframe systems run diverse workloads that typically are complex, comprehensive, information-processing centers. Where highly skilled security management is required from experienced system administrators who are in high demand. And where an approach to security and compliance also relies on capabilities integrated into the mainframe itself. Yet for all these high-end capabilities, dealing with threats in the mainframe silo often occurs only after administrators receive a system alert—if they receive one at all.

In the face of today’s threats, however, this inward-looking approach is not sufficient. All systems, including mainframes, need to be part of the big enterprise picture, with visibility into events across the entire infrastructure. They need to see, for example, where an intruder entered the network, the footprints the intruder left while traversing the network, and the target the intruder is aiming to attack.

But in the mainframe world, administrators typically gather data and generate reports on the threat to their system alone. By contrast, in the SOC world, analysts constantly monitor user behavior across the full network—before, during and after an event—then analyze and report their findings. The challenge is: The SOC has little or no visibility into the mainframe.

Now when mainframe intelligence is combined with SOC intelligence, the mainframe is no longer so isolated. Administrators in the data center and the SOC alike have a better view into all systems, and better control of enterprise security.

70% of organizations cannot report on end-user entitlements for data access.¹

Learn more in this IBM white paper about best practices for mainframe security.

Criminals move fast. Enterprises, not so much. On average, a malicious or criminal attack takes 229 days to discover and 82 days to contain. Data breaches caused by human error are quicker to handle—but not by much—requiring 162 days to find and 59 days to contain. In either case, threats have plenty of time to inflict their damage.

So with the number of sophisticated threats on the rise, rapid response—as close to real time as possible—is more important than ever. The traditional focus of security strategies was to erect perimeter defenses and then react over a period of days or even months when those defenses were breached. Especially in mainframe environments, these management processes were often carried out manually. For timely action against threats, however, today’s focus has shifted to continuous, automated monitoring and remediation.

As enterprise computing has become more diverse and more mobile, the highly-securable mainframe may still be central to enterprise computing and data operations. As such, it is commonly referred to as the “system of record.” But the less securable devices that connect with it—any of which can be an entry point for a criminal attack—mean never-ending vigilance and rapid response to attacks are essential.

A proactive security information and event management (SIEM) solution that can centrally monitor the network, collect data and report on activities affecting both mainframes and the enterprise’s diverse infrastructure—and then integrate with additional capabilities to issue timely alerts to analysts—now becomes critical for responding to security events.

The average company experiences 3.4 security incidents a week.²

---


² IBM X-Force Research, 2016 Cyber Security Intelligence Index, “Reviewing a year of serious data breaches, major attacks and new vulnerabilities,” April 2016.
Integration: Feed data from the mainframe to your SIEM

Breaking down silos isn’t just removing walls. It’s taking what was behind the wall and integrating it with other technologies to empower capabilities that are more effective than previously possible—or that address needs that did not exist when the walls went up. In the case of the mainframe, breaking down silos means the ability to use the system’s security data the same way data from diverse technologies is used.

Whether your mainframe’s enterprise security manager is IBM Resource Access Control Facility (RACF®) or a third-party solution, the ability to integrate its use with the event collection and reporting capabilities of your SIEM solution gives your SOC the ability to effectively consume mainframe security data in a more familiar way. When you use IBM QRadar® SIEM, this integration enables enhanced insight into events on your mainframe—events that previously have been hidden from the SOC but that are vital to comprehensive security intelligence.

The expanded capabilities that integration makes possible allow the enterprise to better address security for the huge range of workloads that mainframes handle—while also addressing the expanding security demands in your enterprise’s diverse computing environment. Many of these needs grow from rapidly expanding mobile, cloud, collaborative and big-data analytics platforms.

Integrated capabilities can help you address these concerns as you adopt security best practices to support industry standards and regulations, reduce the workload of your mainframe administrators by adding SOC capabilities to your mainframe security management, and operate more efficiently and cost-effectively with greater automation.

Integration with QRadar provides broad and deep visibility.

Watch this IBM video for a look inside QRadar.
IBM can manage mainframe and SOC security together

A big-picture, timely, integrated approach that enables managing security for mainframe and diverse computing environments together is an important step toward cognitive computing. Breaking down management silos, opening up visibility into security events and extending security capabilities from the SOC to mainframes helps the security team better understand what’s driving threats, how to combat risk and how to prevent breaches—and get intelligent help in dealing with digital danger.

Combining under one management roof the necessary capabilities for faster and more accurate threat detection, reduction in exposures and vulnerabilities, and expanded insight into events across the infrastructure helps the SOC follow best practices to keep the enterprise secure. From the chief security officer who sets policies to the SOC and mainframe teams that enforce those policies, your security experts can better use data and insight to detect threats, respond to alerts, comply with security regulations, shrink overhead—and, ultimately, reduce risk.

As a leading innovator in today’s cognitive era, IBM Security makes this approach possible with an integrated set of solutions. IBM solutions collect security records, monitor and report on threats and vulnerabilities, create alerts, and analyze events with capabilities that are both mainframe-specific and enterprise-wide.

Now security data collection and reporting expands beyond the mainframe’s long-established RACF capabilities. With new, built-in capabilities, IBM Security zSecure™ Audit collects, formats and sends enriched mainframe audit records to QRadar SIEM to be included in enterprise-wide management, detection and forensics. Mainframe solutions in the IBM Security zSecure suite also integrate with other IBM Security solutions to further break down silos.

To learn more, click on the product name.

The IBM Security zSecure suite helps detect threats, comply with policies and regulations, and reduce costs.
Mainframe environments traditionally use RACF to protect their system resources by controlling what users can do within applications and resources. But mainframe security isn’t just about RACF. IBM now extends capabilities from its broad portfolio of industry-leading security solutions—capabilities previously available only for the SOC—to mainframes.

At the heart of this new approach is the zSecure portfolio of mainframe-focused solutions, now integrated with an enhanced engine that feeds mainframe events into QRadar SIEM, giving you enterprise-wide log management, anomaly detection, incident forensics, and configuration and vulnerability management.

Learn more on the web about the full portfolio of IBM Security solutions.
To guard against data threats of any kind—whether malicious or accidental, internal or external, on a mainframe in the data center or a smartphone in the palm of a user's hand—the security team has to know what's happening on the network. So IBM starts at the beginning, collecting audit records, statistics and environmental data; detecting security exposures; and analyzing exposures for informed action.

And a key new function is the ability to do it all faster than ever. System Management Facility (SMF) records that document activity on mainframes traditionally have been processed in batch format—but new enriched collection capabilities built into zSecure Audit enable streaming in near real time. Mainframe security data now can be processed not only faster but also together with records from the diverse systems managed by the SOC for enterprise-wide resource protection.

IBM solutions work together to provide these capabilities:
- **IBM RACF**—A comprehensive security system that also provides extensive logging and reporting of authorized and unauthorized attempts to gain access to the mainframe and its resources
- **IBM Security zSecure Access Monitor**—Providing statistics for access and authentication usage in RACF to help clean up unused security definitions
- **IBM Security zSecure Alert**—Delivering predefined and customizable alerts for common conditions and events defined according to business requirements
- **IBM Security zSecure Audit**—Helping secure systems by automating security exposure detection and streaming event data it discovers to the SIEM application for real-time processing and more accurate time-stamping of events
- **IBM Security Guardium**—Monitoring sensitive data and threats in databases using real-time threat detection, activity analysis, blocking of suspicious transactions and quarantining of compromised data

Learn more in this interactive IBM white paper about improving mainframe security by cleaning up your RACF databases.
Audit, report and monitor to support regulatory compliance

Being in compliance with regulatory mandates does not necessarily mean being secure. It’s not uncommon to encounter regulations written some time ago that do not incorporate current security best practices.

But compliance is still important, with the proliferation of standards such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), and the new GDPR.

To meet these standards, organizations need security solutions for their entire infrastructure—from mainframes to mobile devices—that ensure maximum visibility into activities within the operational environment, along with automated threat analysis and remediation.

A number of IBM solutions provide these capabilities:

- **zSecure Audit**—Aiding the detection of concealed and complex risks by using a built-in knowledge base to perform extensive automated analysis of the operating system, security system and major subsystems; integrating security event information from critical IBM z/OS® subsystems and applications
- **Guardium**—Scanning database infrastructures to discover sensitive data sources and detect exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges that can cause noncompliance; providing audit capabilities for data at rest and data in motion
- **QRadar**—Consolidating event data from thousands of devices and applications across the infrastructure, uncovering suspected incidents in near real time to support compliance and threat management; employing the advanced IBM Sense Analytics™ Engine to baseline normal behavior, detect anomalies, uncover advanced threats and remove false positives

Learn more on the web about QRadar and Sense Analytics.
Immediately alert your security team when threats occur

Knowing when suspicious activity or actual threats occur on the network is critical—but the effectiveness of threat information is diminished if administrators receive alerts so late that damage is already done, receive so many alerts that they can’t handle them, or receive false-positive data that obscures the real danger. If they have to manually configure systems and software to send those alerts, the added workload can be yet another roadblock that makes managing security difficult. Manual processes can become so complicated that verifying compliance with security regulations also is a challenge.

To help mainframe and SOC administrators achieve more timely and more accurate detection, analysis, alerting and response, new capabilities built into the zSecure suite enable mainframes to feed event data to QRadar SIEM to detect and prioritize potential threats, then produce alerts in near real time. Capabilities such as support for PCI-DSS now built into zSecure Alert are designed to improve compliance verification while streamlining compliance management to reduce the administrators’ workload.

The key solution for providing timely, accurate alerts to mainframe and SOC administrators is:

- **zSecure Alert** — Enabling both predefined alerts for common conditions and customizable alerts to match business requirements; providing immediate and integrated remediation for intrusion attempts; helping reduce costs associated with failed audits or compliance; integrating with other solutions to send real-time alerts to QRadar SIEM to improve insight into threats across the enterprise

*Read the IBM data sheet to learn more about zSecure Alert.*
Keep your mainframe secure with targeted capabilities

Collecting, reporting and alerting are the groundwork for enterprise security, but once administrators have data in hand, it’s important to be able to analyze information to know what it means. On the mainframe, administrators can conduct analysis in two principal ways: using analytics for security-specific data made possible by the zSecure suite of solutions or using broad capabilities for analyzing all data—security-related and otherwise, structured and unstructured—processed by the mainframe made possible by IBM Operations Analytics for z Systems. Adding Guardium to the mainframe security toolkit provides further analytics capabilities for analyzing data stemming from security events and threats to mainframe databases.

Individually and together, these solutions provide a full range of analytics capabilities:

- **zSecure Audit** — Measuring and verifying the effectiveness of mainframe security by analyzing critical information such as SMF log files (to create a comprehensive audit trail) and analyzing RACF profiles (to answer questions such as “Who has access to this data set?” and “Who are the system’s special users who have not changed their password?”)
- **Operations Analytics for z Systems** — Enabling users to search, visualize and analyze data across mainframe operating environments, with operational insights at a glance, and summaries of key operational issues along with actionable advice for accelerating problem investigation and resolution
- **Guardium** — Scanning and analyzing audited data through its Threat Diagnostic Center to detect symptoms indicating that a database attack such as a SQL injection or malicious stored procedures is underway from inside or outside the organization

Explore Operations Analytics for z Systems in a live demo.
Bring together data and innovation to remain secure

Integrating IBM Security solutions for a big-picture, timely response to threats across mainframe and SOC environments delivers time-tested—and client-trusted—capabilities for securing your valuable resources. And it opens the door to the newest innovations from independent developers, business partners and your peers worldwide. This is precisely the combination organizations need today for greater security visibility and control across the entire enterprise—from the data center to your mobile workforce.

For comprehensive enterprise-wide security, the IBM approach now enables mainframes to feed enriched RACF security data into QRadar SIEM for near-real-time identification of security incidents. The innovative IBM Security App Exchange facilitates sharing of applications, application extensions and enhancements for IBM Security products.

- **QRadar SIEM**—Enabling mainframe and SOC security teams to detect unusual behavior, discover threats and avoid false positive findings by consolidating event data from throughout the infrastructure; utilizing advanced Sense Analytics to examine and interpret security information fed into it from the mainframe and diverse computing devices to track incidents and build a history of supporting data that can help administrators understand the nature of threats.

- **IBM Security App Exchange**—Providing a platform through which analysts can research security threats, aggregate intelligence, collaborate with peers and download security applications; making applications available from IBM and third parties to meet requirements such as adding real-time intelligence feeds to QRadar, integrating third-party solutions with QRadar, or providing enhanced user behavior analytics for QRadar.

Learn more in the IBM video about improving security with collaborative defense.
Why IBM?

Gone are the days when specialized point security products could meet all security needs. Now it's time to close remaining gaps and tear down management silos in enterprise security capabilities. It's time to address the entire security platform from the mainframe to diverse computing systems—and secure it all together consistently.

IBM capabilities for collecting information, automating corrective actions, continuously enforcing security policies, and monitoring, analyzing and auditing records provide the enterprise-wide view of threat activities that organizations need to sustain ongoing system and data security as well as regulatory compliance.

Significantly, IBM solutions enable a cognitive approach to security—one where systems administrators' workloads are simplified and security teams better understand what's driving threats, how to combat risk and how to prevent breaches. Cognitive security generates not just answers but recommendations for improved decision making. It gives the enterprise intelligent help in dealing with the growing number and sophistication of threats to valuable enterprise resources.

With IBM, you have the insight and control you need to manage your mainframe environment and your diverse computing environment together, with big-picture visibility into your entire security landscape, the ability to take timely preventive action and respond in real time when an attack occurs, and integrate your security applications to extend the capabilities built into each so you have stronger protection than ever before.

Learn more about IBM Security on the web.
The IBM Security portfolio

Security Operations and Response
- IBM QRadar SIEM
- IBM QRadar Vulnerability Manager
- IBM QRadar on Cloud
- IBM QRadar Incident Forensics
- IBM Resilient Incident Response
- IBM Security Network Protection XGS
- IBM Security Trusteer Pinpoint
- IBM Security Trusteer Mobile
- IBM Security Trusteer Rapport

Information Risk and Protection
- IBM MaxS360
- IBM Security Guardium
- IBM Security Key Lifecycle Manager
- IBM Security AppScan
- IBM Cloud Security Enforcer
- IBM QRadar on Cloud
- IBM QRadar Incident Forensics
- IBM Security Identity Governance and Intelligence
- IBM Security Privileged Identity Manager
- IBM Security Cloud Identity Service
- IBM Security zSecure, IBM RACF, IBM Multi-Factor Authentication for z/OS

Security Transformation Services
Management consulting | Systems integration | Managed security
For more information

To learn more about IBM solutions for protecting against insider threats to enterprise resources, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

About IBM Security

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, provides security intelligence to help organizations holistically protect their 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