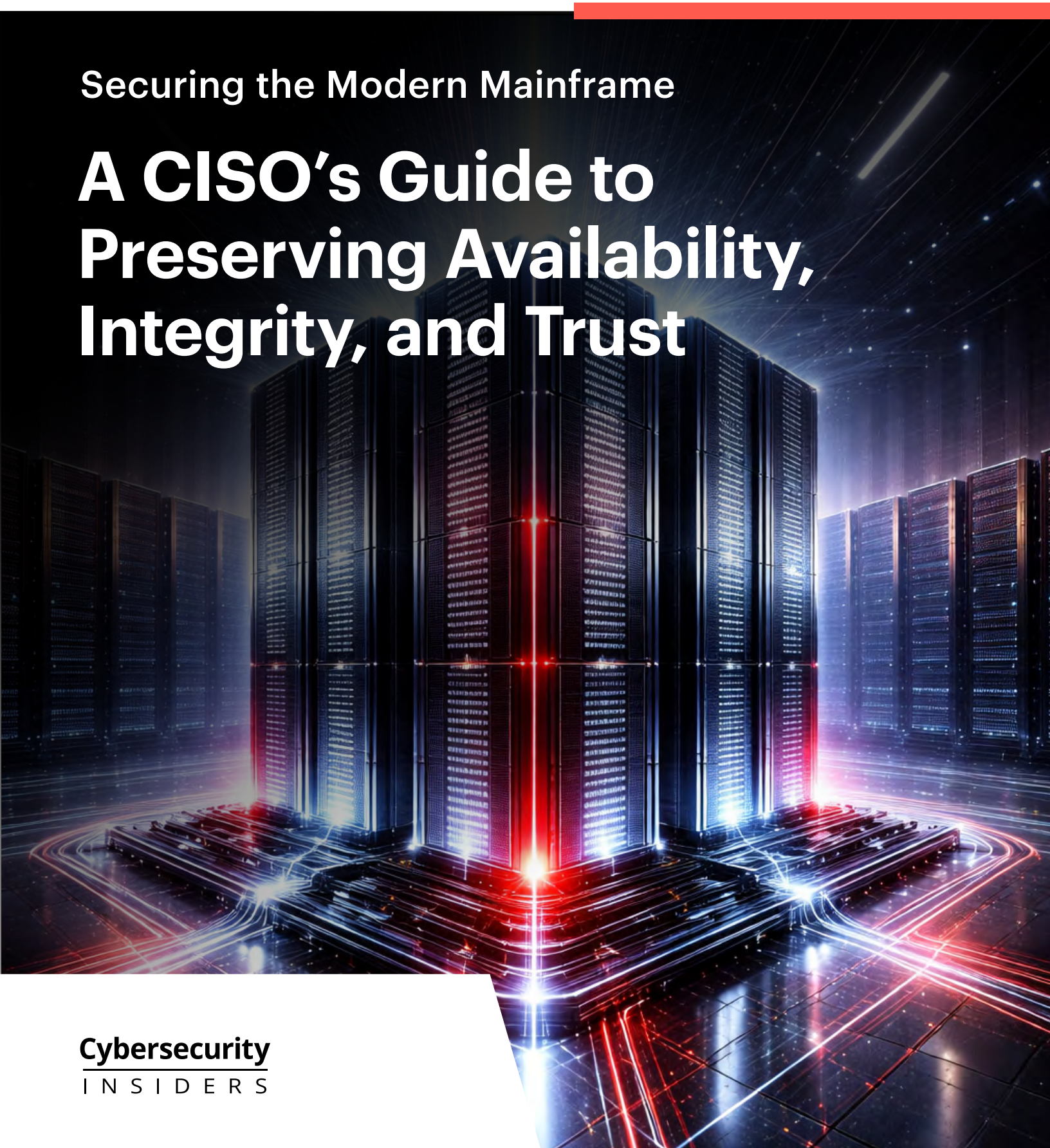
bmc

Securing the Modern Mainframe

A CISO's Guide to Preserving Availability, Integrity, and Trust



Cybersecurity
INSIDERS

Executive Summary

The Moment Everything Stops

At 6:47 AM, overnight batch fails. Within the hour, security operations confirms malicious encryption activity against core production databases. The mainframe, the platform that clears every transaction the business depends on, is now part of the blast radius.

The first question is immediate: what can still be trusted? Which balances are accurate? Which claims are valid? How far back does exposure extend? The mainframe may still be processing, but confidence in its output has collapsed.

Modern mainframe attacks are rarely sudden. Reconnaissance often unfolds quietly for 3–6 months. Attackers map datasets, observe batch cycles, study privileged access, and identify backup schedules long before they encrypt anything. With behavioral monitoring in place, abnormal access patterns can surface during this reconnaissance phase, when containment is still surgical and business impact is minimal. Without it, the first signal may be a ransom demand.

What follows is a framework for intercepting attacks during the reconnaissance phase, and preserving every transaction if an attack succeeds. It draws on BMC's experience securing mainframe environments at the world's largest financial institutions, healthcare organizations, retailers, and government agencies. The 90-day roadmap at the end provides a structured path to measurable progress.

On distributed systems, security failure often appears as outage, degraded service, data exposure, or corruption in a specific application or workflow. On the mainframe, failure strikes closer to the enterprise core: critical operations can stop, transaction integrity can come into question, and the organization can lose confidence in the records it depends on to run the business.

That distinction matters because the mainframe is not simply another compute platform. It is often the transactional backbone for payments, claims, settlements, orders, and account updates. When those processes are interrupted, altered, or cast into doubt, the incident becomes more than a technical event. It becomes a business trust crisis.

The Executive Case: Why Mainframe Security Has Changed

Mainframes did not become vulnerable because they weakened. They became exposed because the enterprise around them changed. Hybrid architectures, API integrations, shared identity infrastructure, automated batch operations, and AI-connected services have extended trust relationships across platforms that operate at different speeds and with very different visibility. Attackers exploit those connections.

Compromise rarely begins on the mainframe itself. It starts with phishing, credential theft, supply chain compromise, misuse of trusted integrations, and abuse of legitimate contractor access, and propagates inward.

The threat is accelerating. GenAI tools speed up reconnaissance and credential harvesting. Ransomware-as-a-Service enables sophisticated attacks via automated platforms. Nation-state actors stage dormant malware, waiting for a geopolitically opportune moment to strike. Adversaries even place operatives inside organizations through seemingly legitimate employment, gaining trusted access from day one. Recent DOJ indictments highlight adversaries running "laptop farms" to secure IT roles, harvest credentials, and operate within enterprise environments as authorized users.

Recent successful attacks involving mainframe environments have disproportionately relied on credential theft, insider misuse, or abuse of trusted access paths. Attackers do not need deep z/OS expertise if they can authenticate and operate within existing permissions. Once inside, their activity often appears legitimate to traditional access controls that verify whether access is permitted but not whether behavior aligns with business intent. Executive accountability has shifted to match: resilience is now measured by demonstrable detection, containment, and recovery capabilities across availability, integrity, and data exposure risks. The question has evolved from "Was access authorized?" to "Can you preserve operational continuity and trust under attack?"

Because the mainframe is often the system of record for payments, claims, orders, balances, and other business-critical transactions, the impact of compromise is not limited to infrastructure disruption. Availability loss halts operations. Integrity loss undermines confidence in what the system is reporting. Confidentiality loss exposes regulated data and creates leverage for extortion. In practice, these risks converge at the system of record, where technical compromise becomes a business trust problem.

The reconnaissance window is both the attacker's advantage and your opportunity.

Adversaries often spend weeks or months observing activity, mapping datasets, and identifying high-value access paths before acting. With the right visibility, that dwell time becomes detection time. Understanding how these attacks unfold in practice requires looking beyond individual controls and examining the structural conditions that allow them to succeed.

How Mainframe Attacks Succeed

Mainframe security incidents rarely succeed because a control was entirely missing. They succeed because the system behaves exactly as designed, but under conditions it was never built for: trusted access, extended integrations, and visibility gaps that allow malicious behavior to blend into normal operations.

Six structural breakdowns recur across industries and investigations, creating the conditions for attackers to operate undetected and escalate impact:

1 The mainframe is invisible when risk emerges

Security telemetry is processed hours after the fact, reviewed by specialists outside the SOC, and disconnected from enterprise incident-response workflows. Reconnaissance activity (dataset scanning, catalog exploration, JCL inspection) generates no real-time alerts. Adversaries map the environment unobserved. As a result, early reconnaissance, abnormal access patterns, and data exploration activity often go undetected during the phase when intervention would be least disruptive.

2 Legitimate access becomes the attack path

Service accounts, contractor identities, and inherited permissions created for one-time tasks often retain elevated privileges for years. When credentials are stolen, attackers inherit accumulated access and operate entirely within authorization boundaries. Every action looks legitimate because, technically, it is. Attackers do not need to bypass controls if they can operate within them, using access that appears valid but exceeds what is actually required.

3 Enterprise governance drifts from mainframe reality

Zero trust architectures assume continuous identity verification and dynamic access adjustment. The mainframe, with its batch-oriented security model, often grants standing access to service accounts created years ago. The CISO's dashboard may show "zero trust implemented" while the mainframe tells a different story. This disconnect is amplified by non-human identities, long-lived certificates, and service accounts that are rarely reviewed but often hold broad access.

4 Compromise cannot be scoped fast enough

Determining what was accessed, altered, or staged is slow and difficult. Without timely forensic visibility, organizations either shut down broadly (halting legitimate operations) or under-respond (allowing the attack to continue). This delay is particularly critical because it extends uncertainty not only about system integrity, but also about whether sensitive data was accessed or exfiltrated during the attacker's dwell time.

5 Containment means disruption

Isolation options on the mainframe are blunt. The surgical precision available on distributed platforms (quarantining a container, isolating a network segment) often does not exist without deliberate architectural preparation. Without precise visibility into affected workloads and identities, organizations often face a tradeoff between halting critical operations or allowing potentially compromised activity to continue.

6 Modernization creates new attack paths

APIs, mobile and web integrations, AI-connected services, and adjacent modernization efforts increasingly expose the mainframe through interaction paths that were never part of its original security model. These connections can reuse credentials, inherit weak trust assumptions, or bypass outer layers of control, giving attackers more direct access to applications and data without needing deep mainframe expertise.

These patterns reinforce each other. An attacker compromises credentials, operates invisibly, exploits governance gaps, and uses extended access paths to study the environment before acting.

By the time the incident is detected, the inability to quickly determine what was accessed, altered, or exposed can paralyze the response.

Organizations are forced to choose between continued operation and decisive containment, often without full confidence in the integrity or confidentiality of their data.



The Architecture: Three Pillars of Mainframe Resilience

DETECT	GOVERN	RECOVER
REDUCE DWELL TIME	REDUCE BLAST RADIUS	REDUCE MEAN TIME TO RECOVERY
Real-time SIEM Integration BMC AMI Command Center for Security	**Time-Bound Privileged Access** BMC AMI Security	**Immutable Backup (3-2-1)** BMC AMI Cloud
Behavioral Analytics & EUBA BMC AMI Security	**Enterprise MFA Integration** BMC AMI Security	**Transaction Log Streaming** BMC AMI Data
Automated Threat Response BMC AMI Security	**Non-Human Identity Governance** BMC AMI Security	**Forward Transaction** BMC AMI BMC AMI Data
Forensic Analysis BMC AMI Security	**Certificate Lifecycle Management** BMC AMI Security	**File Integrity Monitoring** BMC AMI Security
	Network Micro-Segmentation BMC AMI Security + Illumio	

Preserving mainframe resilience takes three capabilities that work together: the ability to detect threats early, govern access continuously, and recover operations in a trusted state.

Each pillar addresses a specific failure mode observed in real-world attacks: lack of visibility during reconnaissance, uncontrolled access through legitimate identities, and inability to restore operations with confidence. When these capabilities operate together, they allow organizations to detect threats early, limit their impact, and restore business trust when incidents occur.

PILLAR 1

Detect – Real-Time Visibility, Context, and Response

You can't stop what you can't see. Mainframe telemetry must flow into the SOC in near real time, normalized alongside distributed events, so risk is assessed in enterprise context, not in a silo. But visibility alone is not enough. Detection must focus on behavior: identifying reconnaissance, abnormal access patterns, bulk data activity, and misuse of legitimate credentials early enough to interrupt the attack before it impacts operations or sensitive data.

Enterprise SIEM integration

BMC AMI Command Center for Security delivers native integration with Splunk, IBM QRadar, Microsoft Sentinel, and other enterprise SIEM platforms, bringing mainframe signals into existing SOC workflows. Mainframe alerts appear in the same dashboards analysts already use, with pre-built correlation rules for z/OS security events. SOC analysts triage mainframe incidents without requiring deep z/OS expertise.

Behavioral analytics

Because attackers using stolen credentials often operate within authorized boundaries, rule-based detection alone is insufficient. BMC AMI Security's AI-driven behavioral analytics establish baselines for what "normal" looks like for each identity and workload, then flag deviations in real time across z/OS subsystems, identity controls, and network activity. These deviations often appear first during reconnaissance, when attackers explore datasets, test access paths, or begin staging data for extraction. A preloaded database of vulnerability use cases and indicators of compromise extends detection coverage from day one.

Automated response

Human response is measured in minutes—at best—while attack progression unfolds in seconds. BMC AMI Security closes that window with honeypot datasets that trigger immediate session termination on access, session freezing for anomalous encryption or bulk data activity, and real-time notification to incident ticketing and collaboration platforms. Early, automated intervention is critical to limiting both operational impact and potential data exposure.

Forensic analysis

When incidents occur, BMC AMI Security's forensic dashboards provide high-speed indexed search across massive volumes of SMF, Db2, and JES data, enabling analysts to pinpoint "patient zero" in seconds rather than days. Critically, forensic analysis happens off-platform, on systems not affected by the attack. This speed is essential not only for containment, but for determining whether data was accessed, altered, or exfiltrated during the attacker's dwell time.

PILLAR 2

Govern – Continuous Identity Access Control

Detection reveals the threat. Identity and access governance determine how much damage that threat can do. When attackers compromise a credential, the blast radius is defined by what that identity can reach. On many mainframes, the highest-risk identities are not only individual users but also service accounts, batch identities, inherited entitlements from acquired environments, long-lived certificates, and other non-human access paths that retain broad privileges with limited oversight. Governance must extend across all of them.

Time-bound privilege
Standing privilege is standing risk. BMC AMI Security enforces time-bound access by default with automatic expiration, ensuring attackers who compromise credentials inherit only what is active at that moment, not years of accumulated grants. Limiting standing privilege reduces not only unauthorized access risk, but also the effectiveness of credential theft and insider misuse.

Enterprise identity integration
Step-up multi-factor authentication should apply to high-risk actions and integrate with enterprise identity providers across the broader environment. Certificate lifecycle automation handles renewal as validity windows shrink, reducing outage risk while limiting the exposure created by long-lived machine-to-machine trust relationships.

Non-human identity governance
Batch and service accounts must be governed with the same rigor as users, often more, since they carry broader access with less scrutiny. The same applies to API identities, certificates, and other machine-to-machine access paths that connect modern applications to the mainframe. BMC AMI Security provides continuous governance with automated certification for these identities.

Network micro-segmentation
Zero trust extends beyond identity to network architecture. Integration with platforms like Illumio brings micro-segmentation to z/OS. This reduces lateral movement even when attackers gain legitimate access through identity-based entry points.

PILLAR 3

Recover – Trusted Recovery of Workloads and Transactions

Prevention reduces probability. Recovery defines resilience. On the mainframe, recovery is not just about restoring systems, but restoring confidence in the workloads, data, and transactions the business depends on.

On systems of record, the executive metric that matters most is Mean Time to Recovery, measured not only in hours but in transaction confidence. Can you restore operations quickly, recover trusted transaction history, and avoid giving attackers leverage over the business? That is the question boards, regulators, and customers will ask.

Recovery does not eliminate exposure. Even when systems and transactions can be restored, organizations must determine whether sensitive data, executive communications, or regulated records were accessed or exfiltrated during the attacker's dwell time. Without that understanding, recovery may restore operations but not trust.

The problem with traditional recovery

If the last clean backup was taken at midnight and the attack is detected at 4 PM, the organization faces a critical gap: the production system may be compromised, but 16 hours of legitimate business activity still needs to be recovered in a trusted way. Without isolated logs, immutable backups, and forward recovery, those transactions may be delayed, disputed, or effectively held hostage by the incident.

Immutable backups

BMC AMI Cloud implements the 3-2-1 principle: three copies, two media types, one off-site, all beyond attacker reach. Immutable backups cannot be altered or destroyed, even by administrators with compromised credentials. Backup frequency determines maximum exposure, but on the mainframe the objective extends beyond restore speed. It is to preserve a trusted baseline from which operations and transaction history can be rebuilt with confidence.

Transaction recovery

BMC AMI Cloud streams database logs for Db2, IMS, and VSAM continuously to an immutable vault via secured, out-of-band paths using WORM technology. After restoring from the last known-good backup, the organization replays every legitimate transaction up to the moment the attack began. The attacker's leverage collapses: access to your transaction history is no longer scarce. This capability restores not just data, but confidence in the sequence and completeness of business operations.

Malware identification and removal

Ransomware is typically staged weeks or months before execution. File Integrity Monitoring identifies which programs were modified or introduced, so teams can surgically remove malware before operations resume. This ensures that restored environments are not only operational, but free of latent threats that could reintroduce risk.

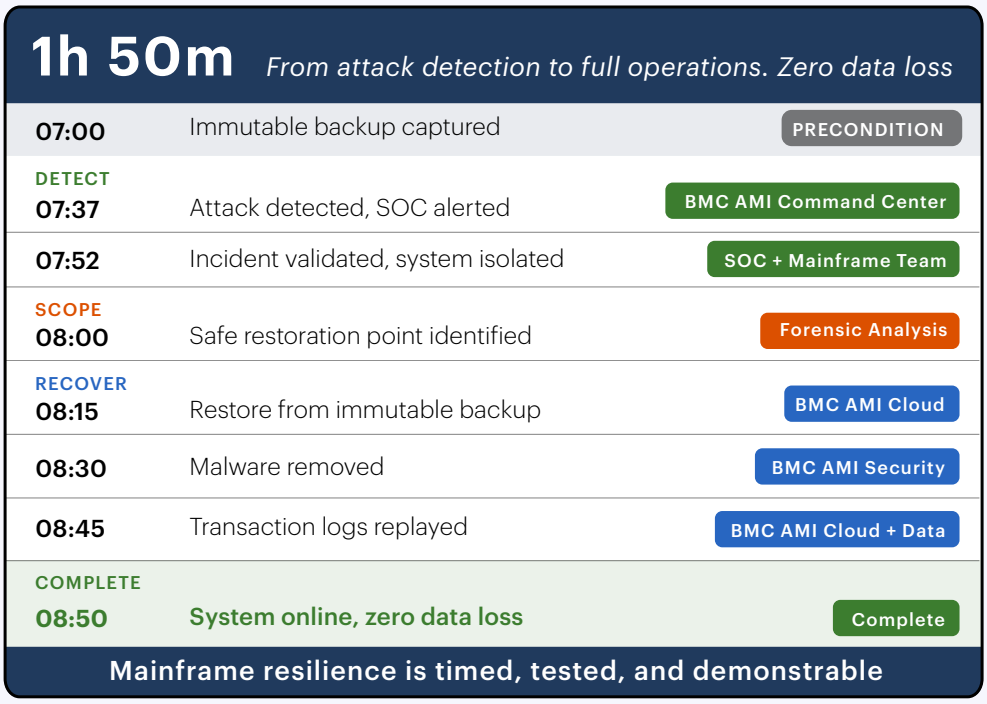
Demonstrated Recovery: Under Two Hours, Zero Data Loss

Attack Lifecycle

Reconnaissance 3-6 Months *Your detection window*	Access & Staging Weeks	Encryption & Disruption Minutes	Recovery <2 Hours
ATTACKER ACTIVITY Map datasets and privileged accounts, study batch cycles and backup schedules	**ATTACKER ACTIVITY** Escalate privileges, install dormant malware, establish persistence	**ATTACKER ACTIVITY** Encrypt production databases, destroy accessible backups, deliver ransom demand	**ATTACKER ACTIVITY** Ransom demand fails. No leverage
WHERE ATTACKS ARE STOPPED			
DETECT **Behavioral Analytics** Baselines flag unusual dataset scanning and access patterns DETECT **SIEM Integration** Real-time telemetry surfaces reconnaisance to SOC	GOVERN **Time-Bound Privilege** Limits inherited access from compromised credentials GOVERN **Non-Human Identity Governance** Service accounts governed with automated certification DETECT **Honeypot Datasets** Immediate session termination on unauthorized access	DETECT **Automated Response** Session freezing halts encryption in seconds GOVERN **Micro-Segmentation** Blocks lateral movement across subsystems DETECT **Forensic Analysis** Pinpoints safe restoration point in seconds	RECOVER **Immutable Backups** Restore from copies beyond attacker reach RECOVER **Transaction Recovery** Replay transactions with zero data loss RECOVER **File Integrity Monitoring** Surgical malware removal before operations resume

The following sequence illustrates how detection, containment, and recovery operate together to restore a trusted state.

TIME	ACTIVITY	BMC CAPABILITY
07:00	Immutable backup captured	BMC AMI Cloud
07:37	Attack detected, SOC notified	BMC AMI Command Center
07:52	Attack validated, mainframe isolated	SOC + Mainframe Team
08:00	Safe restoration point identified	Forensic Analysis Dashboard
08:15	Restore from immutable backup	BMC AMI Cloud
08:30	Malware removed via FIM	File Integrity Monitoring
08:45	Transaction logs replayed	BMC AMI Cloud + BMC AMI Data
08:50	System online, Zero Data Loss	Complete



Elapsed from detection (07.37) to full operations (08:50): 1 hour 13 minutes

Mainframe resilience must be timed, tested, and demonstrable.

On a system of record, assumed recoverability is not enough.

Three Questions to Test Your Readiness

The "Tuesday" Test (Recovery): *"If ransomware hit today and we had to restore from Tuesday's backup, how specifically would we replay the transactions that happened between Tuesday and now? Are those logs isolated and protected, or could they be compromised along with the primary system?"*

The "Silent Admin" Test (Visibility): *"If a contractor with valid credentials downloaded 5,000 sensitive records outside normal batch hours, would the SOC get an alert immediately, or find it in a report next week? Would we recognize that behavior as abnormal in real time, or only after the fact?"*

The "Forever Access" Test (Governance): *"Can you show me a list of all external service accounts active for more than 12 months, and the date each was last recertified?"*

If any of these questions produce hesitation, the blind spot is real.

Why the Problem Persists: The Friction Behind Inaction

If these risks are well understood, why do blind spots persist? Because organizational friction persists. The result is inertia, driven by four forces:

- **Funding gaps:** Mainframe costs sit with infrastructure teams, not CISO budgets. Security improvements fall between budget owners.
- **Toolchain fragmentation:** Mainframe telemetry requires specialized parsing. SIEM integrations demand custom development that competes with higher-priority initiatives.
- **Skills scarcity:** Mainframe expertise is concentrated in a shrinking specialist population, separate from security operations. Neither team has capacity to learn the other's domain.
- **Change risk aversion:** "If it's working, don't touch it" is culturally reinforced by decades of operational success, even when modern solutions deploy non-invasively.

Any credible architecture must address these realities: pre-built SIEM connectors (no custom integration), normalized alerts usable by existing SOC staff (no z/OS expertise required), non-invasive deployment (no production changes), and licensing that fits existing budget structures. These barriers persist even as attack paths evolve, which is why improvements in visibility, identity governance, and recovery must be achievable without disrupting core operations.

Metrics That Matter

These metrics reflect the organization's ability to detect threats early, constrain their impact, and restore operations with confidence.

METRIC	WHAT IT MEASURES	BMC IMPACT
Mean Time to Detect (MTTD)	How quickly the SOC identifies mainframe anomalies	Target: <15 min with SOC-integrated telemetry
Standing Privilege Ratio	How much risk accumulates through legitimate access	Target: <5% of admin IDs with standing access
Mean Time to Recovery (MTR)	How fast operations resume with trusted data, transactions, and business continuity	Demonstrated: <2 hours, zero data loss

A 90-Day Roadmap

The following roadmap establishes meaningful progress within a single quarter. The sequencing is deliberate: observe first, govern next, validate recovery last.

PHASE 1

Establish Visibility (Weeks 1–4)

Deploy BMC AMI Command Center for Security with SIEM integration. Configure out-of-box indicators of compromise for z/OS, Db2, CICS, and RACF/ACF2. Establish behavioral baselines for privileged users. Validate that SOC analysts can triage alerts without calling a mainframe expert. This establishes the foundation for detecting reconnaissance and abnormal behavior before impact occurs.

Proof point: SOC dashboards include mainframe activity. Anomalies triaged in minutes.

PHASE 2

Introduce Guardrails (Weeks 5–8)

Pilot time-bound privilege for highest-risk accounts. Deploy MFA integration via enterprise identity provider. Configure honeypot datasets and test automated response in monitor mode. Inventory non-human identities and classify by risk. This phase reduces the blast radius of identity-based attacks and limits the damage from compromised credentials.

Proof point: Standing privilege reduced 30%+ for high-risk accounts. Automated response tested. MFA deployed to >50% of privileged users.

PHASE 3

Validate Resilience (Weeks 9–12)

Deploy BMC AMI Cloud immutable backup infrastructure. Configure BMC AMI Data transaction log streaming to immutable vault. Test full recovery scenario: backup restore plus transaction replay. Conduct tabletop exercise with executive team. This validates not only system recovery, but the ability to restore trusted operations without uncertainty.

Proof point: Recovery time validated through actual test (target: <4 hours). Transaction recovery demonstrated with near-zero data loss. Executive team has rehearsed ransomware decision-making.

Building Internal Support: Three Tactics That Work

- **Lead with visibility, not control**
  Mainframe teams fear disruption. Win trust by guaranteeing that Phase 1 is strictly non-invasive. Demonstrate value before asking for access governance changes that may feel threatening.

- **Quantify the current blind spot**
  Ask: "How long would it take us to detect a compromised credential on the mainframe today?" If the answer is "hours," "days," or "we don't know," the case makes itself.

- **Start with undeniable use cases**
  No one argues that contractor access should be permanent, that emergency credentials should never expire, or that backups should be accessible to attackers. Start there.

NEXT STEP:
Assess Your Readiness

BMC offers a Mainframe Security Readiness Assessment that evaluates your detection, identity governance, and recovery capabilities, identifies gaps across the modern attack surface, and delivers an implementation plan specific to your environment.

To schedule a Readiness Assessment, contact your BMC account representative or visit **bmc.com/ami-security.**

KEY TAKEAWAYS

Mainframe security is no longer just about preventing compromise. It is about preserving availability, integrity, confidentiality, and business trust when modern attack paths inevitably reach the system of record.

1 Trusted access is the primary attack path

Most meaningful risk now enters through identities, service accounts, integrations, and inherited permissions that appear legitimate until behavior proves otherwise.

2 The reconnaissance window is your advantage

Attackers often spend weeks or months observing environments before acting. With the right visibility, that dwell time becomes detection time.

3 Transaction integrity is the defining mainframe consequence.

When payments, claims, balances, or orders can no longer be trusted, the incident becomes a business integrity crisis.

4 Recovery must restore confidence, not just uptime.

Immutable backup and transaction replay reduce ransom leverage, but organizations must still determine what was exposed and what can be trusted.

5 Start with visibility.

It is the least disruptive first step and reveals the blind spots that make identity risk, modernization risk, and recovery gaps visible.