bmc Mainframe Services
by RSM Partners

Datasheet

Security Services

Secure and harden your mainframes against threats and zero-day vulnerabilities

OVERVIEW

Over 80% of Enterprises say they have the right tools to actively secure the mainframe but only 41% are taking the steps to actively secure it.[1] Tools require the right expertise to make them effective.

BMC's IBM® Z® global security team have the experience to help you uncover the current state of your mainframe security, recommend improvements to harden it against attacks and help you proactively address new threats. From in-depth Security Assessments and Health Checks to Penetration Testing, Vulnerability Assessments and Security Hardening programs, clients worldwide depend on BMC Mainframe Services by RSM Partners to help them work in smarter and more secure ways.

SPECIALIST MAINFRAME SECURITY ASSESSMENT

What you can't see, you can't secure

Mainframes are often audited by organizations or people with little or no knowledge of the required technical depth, who instead perform simple checklist audits. As a result, organizations can incorrectly believe their systems are secure. In fact, over half of enterprises who perform audits report still uncovering security issues.[2]

Gain a complete view
Uncover weaknesses & vulnerabilities
Reduce risks

Specialist Mainframe Security Assessment

By contrast, our in-depth technical assessment of your mainframe security infrastructure, policies and procedures will help you to:

- Gain a complete view of your security posture including every essential security control.
- Uncover weaknesses and vulnerabilities in your configuration, software and controls so you can plug gaps in your defenses.
- Reduce the risk of malicious attacks and data loss – and the reputational damage and financial penalties that can follow.

PENETRATION TESTING

Reveal vulnerabilities and harden your posture against attack

Real world penetration tests have shown that the average mainframe has more than 100 vulnerabilities and can be compromised in minutes. The responsibility for detecting these vulnerabilities lies with you: you need to pinpoint the gaps and take focused action to remedy them. We have the skills, experience and tools to test your defenses for all eventualities.

BMC's penetration testing team acts in the same way an attacker would in order to proactively identify vulnerabilities that could lead to a compromise. Once discovered, they are reported with recommended remediation steps to prevent them from being exploited. The steps of a typical penetration test are:

- Kick-off meeting, planning and scoping.
- Non-disruptive data collection.
- Penetration testing.
- Software scanning.
- Initial findings onsite for time-critical security alerts.
- Final report and checklist for remedial activity.
- Demonstrations of security failings and access achievement.

[1] Source: *A False Sense of Mainframe Security* – a commissioned study conducted by Forrester Consulting on behalf of BMC Software, July 2020
[2] Ibid.

SECURITY-AS-A-SERVICE

On-demand security engineering, management and administration

Organizations without in-house mainframe security expertise or staff can elect to leverage our team with this service. Managed 24/7, we deliver the skills, experience and coverage to help you secure, optimize and continuously protect your systems. You choose and use the elements you want and retain control of your environment. Options include:

- **Security Administration** – maintain a secure environment for critical applications and data while controlling and reducing management overheads.
- **Security Engineering** – designing security tools and structures to mitigate operational risks, combat internal and external threats and combat sophisticated cybercrime and hacking.
- **Software Management** – reduce costs and complexity while making better use of existing security tools.
- **Compliance** – ensure your organization complies with the latest industry and regulatory requirements such as the General Data Protection Regulation (GDPR), PCI, Sarbanes Oxley and ISO standards.
- **Cryptography** – software and hardware-based processes to help you protect sensitive and confidential data, including pervasive data encryption.
- **Staff Augmentation** – address mainframe and security skills gap, deliver projects on time and on budget, and reduce reportable full-time employee (FTE) statistics.

WANT TO LEARN MORE?

We are ready to support your organization and augment your teams with services designed to run, maintain, secure and support your mainframe systems in more focused and cost-effective ways.

FOR MORE INFORMATION

To learn more, please visit **bmc.com/mainframeservices**

KEY SERVICES

- **Independent Consulting** – leverage our objectivity, expertise and experience for any aspect of your IBM® Z® security.
- **Security Health Check** – an intensive best practice check, the key to understanding and protecting against external cyberattacks, internal threats, data leakage, and loss.
- **Penetration Testing** – identify vulnerabilities so you can plug the gaps and strengthen defenses.
- **Security Best Practice** – advice and consulting on digital transformation, the threat landscape, latest thinking and best practices in security.
- **Security Monitoring** – build, deploy and exploit solutions such as zSecure Alert, Splunk and QRadar.
- **Security Remediation** – proactively avoid potentially ruinous breaches affecting your operations and reputation.
- **Software Security Suite** – improved protection and easier security management using packaged software tools you won't find anywhere else.
- **RBAC Implementation and Data Classification** – enabling a key aspect of Z security best practice.
- **Migrations** – V2V migrations and specialist in-house tooling to speed and de-risk ESM migrations.
- **Implementing Security Tools** – install, customize and train your teams in major security toolsets including zSecure and Vanguard.
- **User Provisioning and Recertification** – integrating Z environments with products including Oracle and Tivoli Identity Manager.
- **Compliance** – scan your Z estate to detect the presence of sensitive data specified in various regulations that must be properly managed across the enterprise.

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

www.bmc.com