

Why Mainframe Security Matters For Financial Services Firms

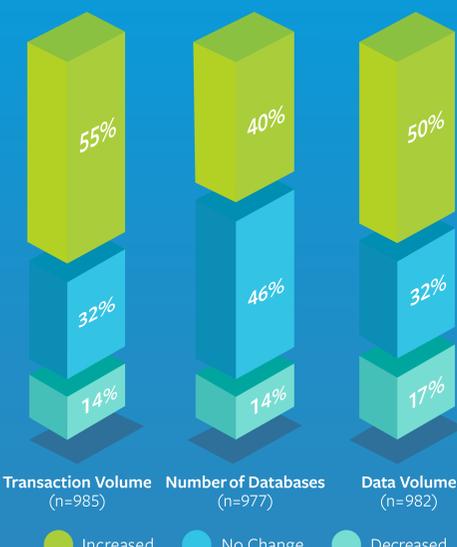


Don't Let Mainframe Be The Gap In Your SecOps Strategy

Financial services firms house much of their critical data on the mainframe and face a growing number of sophisticated cyber threats. Too often a company's mainframe is disconnected from its main security operations center (SOC), leaving the mainframe unprotected. Securing your mainframe should be a business priority. See how you can start securing your high-value data today.

Firms Are Struggling With Mainframe Security Concerns

Whether executives or tech staff, business respondents in BMC's comprehensive 2019 Mainframe Survey report concerns around compliance issues, security, and vulnerability management—yet many firms don't have measures in place to effect change.



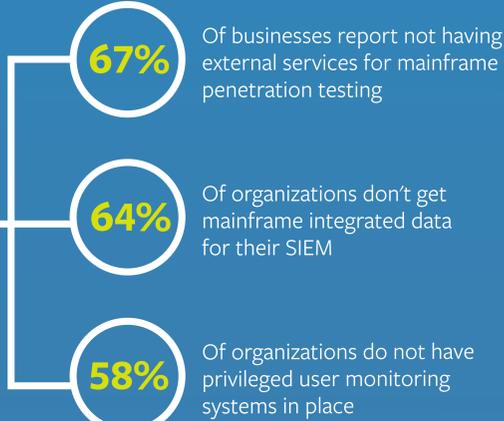
Rapidly Evolving Demands Increase Mainframe Vulnerabilities

As firms work towards solving these security concerns, mainframe workloads, data, and transaction volumes are all increasing exponentially. The MIPS forecast is at its highest level since 2011.

The platform is increasingly relied upon to handle the demands of the digital business environment.

Companies Are Operating With Obvious Security Blind Spots

Mainframes can be hacked **remotely** which makes stringent testing and event management non-negotiable. Customers put their trust in organizations to keep their data secure, but **too few organizations have systems in place** to identify vulnerabilities and breaches before they become a serious liability.



The Cost Of A Data Breach Can Be Significant

The financial and reputational costs of a large scale data breach are significant, particularly in the financial services sector.

\$400,000,000

The total cost for Capital One after a data breach saw them lose private data of 100 million customers¹

\$1,400,000,000

Estimated legal costs and damages paid by Equifax after losing data of 146 million of their customers²

~200

Average number of days to identify a security breach³



Protect Your Business Now With Intelligent Mainframe Solutions

With **BMC AMI for Security**, our Automated Mainframe Intelligence security solution, you can leverage automation domain expertise and predictive analytics to secure your most valuable IT asset and meet evolving compliance requirements. BMC AMI for Security allows businesses to:

- Integrate the mainframe with enterprise security information event monitors (SIEMs)
- Get real-time alerts on mainframe indicators of compromise
- Leverage intelligent IBM® Db2® and IBM® IMS® database activity monitoring
- Automate incident response to cyber threats
- Maintain regulatory compliance with a single audit trail
- Monitor all privileged users

Discover how BMC can help run and reinvent your business and protect your critical data with real-time, automated mainframe coverage.

Learn more now at

www.bmc.com/it-solutions/bmc-ami-mainframe-security