Mainframes and Security: Current Trends, Key Capabilities

ABERDEEN

bmc
Executive Summary

Aberdeen’s analysis of a survey of more than 1,000 organizations using mainframes shows that they continue to have a positive, growth-oriented, and strategic position within the enterprise computing infrastructure.

Given their significant value, it comes as no surprise that mainframe security is identified as a top priority — particularly in the areas of protecting valuable and regulated data and adding capabilities for protection, detection, and response in the mainframe operating environment.

Mainframes in Context: Current Trends

For thousands of organizations worldwide, mainframes continue to be the reliable, tireless workhorses of enterprise computing infrastructure — with a strongly positive outlook for continued growth in computing capacity, databases, application workloads, and transactions.

For example, Aberdeen’s analysis of a survey of more than 1,000 organizations currently using mainframes found that:

- **A net +43%** of all respondents perceived their mainframes as a platform for growth in attracting new workloads (+67% for the Best-in-Class; +30% for Laggards)

- **A net +57%** of all respondents projected growth in general-purpose computing capacity for their mainframes (+66% for the Best-in-Class; +44% for Laggards)

- **Nearly half (47%)** of all respondents host more than half of the organization’s data on their mainframes (61% of the Best-in-Class; 37% for Laggards)

The Aberdeen maturity class framework is comprised of three groups of survey respondents, classified based on their self-reported results across analyst-selected performance metrics:

- **Best-in-Class** (top 20% of all respondents)
- **Industry Average** (middle 50%)
- **Laggards** (bottom 30%)

Net +100% means that all respondents answered positively;

Net -100% means that all respondents answered negatively.

Generally, net +50% or higher is considered a strongly positive indicator.
Mainframes and Security: High Risk, High Priority

Given their significant value to the organization, it comes as no surprise that mainframe security was first among the top three priorities over the next 12 months (see Figure 1). Adding advanced capabilities for intelligence and automation (e.g., artificial intelligence, machine learning) was also at the top, along with cost optimization initiatives.

Security for mainframes is a top priority, for good reason. For example, empirical evidence consistently shows that successful data breaches are 2- to 4-times more likely to occur for data on back-end systems than for data on endpoints (see Figure 2). It’s only logical that attackers find enterprise data on back-end systems to be the most attractive data assets to target — these are typically the organization’s “crown jewels.”
The likelihood of a successful data breach against back-end systems also varies significantly by industry, particularly as seen in recent years in the Accommodation, Healthcare, and Retail sectors (see Figure 3).

**Figure 3: The Likelihood of Achieving a Successful Data Breach is High, Particularly in Accommodation, Healthcare, and Retail**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Servers 2020</th>
<th>Servers 2019</th>
<th>Servers 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>53.8%</td>
<td>64.1%</td>
<td>51.3%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>24.7%</td>
<td>33.1%</td>
<td>37.1%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>73.8%</td>
<td>73.3%</td>
<td>81.9%</td>
</tr>
<tr>
<td>Financial</td>
<td>25.3%</td>
<td>16.2%</td>
<td>15.3%</td>
</tr>
<tr>
<td>Accommodation</td>
<td>73.3%</td>
<td>80.9%</td>
<td>95.3%</td>
</tr>
</tbody>
</table>

Empirical Likelihood (confirmed data breaches/investigated incidents)

*Data adapted from Verizon Data Breach Investigations Report 2018-2020; Aberdeen, February 2021*

At a more granular level, survey respondents identified their **top priorities for mainframe security**, which fall into two main groups:

1. **Mainframe data protection**
   - Achieving and sustaining compliance (e.g., PCI, GDPR, HIPPA, many others)
   - Protection of production data in testing environments
   - Identification and encryption of sensitive data

1. **Mainframe protection, detection, and response**
   - Incident response and recovery
   - Security audit and configuration
   - Integration with security information and event management (SIEM) systems
   - Management of privileged users
   - Behavioral analytics
Mainframes and Security: Key Capabilities, Opportunities

By comparing selected capabilities and performance metrics across the three maturity classes, Aberdeen generated some useful insights about current best practice — and future opportunities — in mainframe security. For example, Best-in-Class organizations are more likely to deploy Pervasive Encryption in their data protection strategies (see Figure 4).

**Figure 4: Best Practices in Mainframe Security — Best-in-Class Organizations are More Likely to Deploy Pervasive Encryption**

![Figure 4: Best Practices in Mainframe Security](image)

Source: Data adapted from BMC Mainframe Survey 2020 (N = 1,081); Aberdeen, February 2021
In addition, leading performers are significantly more likely than lagging performers to deploy a number of key capabilities for **protection**, **detection**, and **response** in the mainframe operating environment (see Figure 5).

**Figure 5: Best Practice in Mainframe Security — Best-in-Class Organizations are More Likely to Deploy Key Capabilities for Protection, Detection, and Response**

The capabilities in Figure 5 are strongly correlated with the achievement of Best-in-Class results — and no wonder, as they tie back directly to the priorities and risks discussed above.

Said another way, these capabilities are strongly correlated with the achievement of Best-in-Class results —and no wonder, as they tie back directly to the priorities and risks discussed above.

Aberdeen’s analysis of the survey results also identified opportunities for future improvements in protection, detection, and response; for example:

- **Faster time-to-detect issues**: Across more than 1,000 organizations, the mean time to detection ranged from 0 to 8 hours (median: about 1.5 hours).

- **Faster time-to-identify the cause of issues**: As a percentage of the total time spent on technical issues, a median of about 37% was to identify the root cause.

- **Faster time-to-identify solutions**: As a percentage of the total time spent on technical issues, a median of about 31% was to identify an appropriate solution.

In multiple dimensions, reducing security-related risks has become a race against **time** — for example, the ability of defenders to detect, respond, and remediate more quickly to security incidents than the attacker timeline for compromising systems and exfiltrating valuable or regulated data.
Summary and Key Takeaways

Putting it all together, a high-level checklist of key capabilities / solution selection criteria for mainframe security is summarized in Table 1.

Table 1: High-Level Checklist of Capabilities for Mainframe Security

<table>
<thead>
<tr>
<th>Key Capabilities</th>
<th>Contributions to Mainframe Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pervasive Encryption</td>
<td>- Protect the significant percentage of high-volume, high-value data hosted on mainframes</td>
</tr>
<tr>
<td>Automated detection and response</td>
<td>- Identify and contain malicious activities before your system is compromised</td>
</tr>
<tr>
<td></td>
<td>- Identify system vulnerabilities before they are exploited</td>
</tr>
<tr>
<td>Integration with leading SIEM solutions</td>
<td>- Support real-time visibility into mainframe activities</td>
</tr>
<tr>
<td></td>
<td>- Identify and alert on anomalous behaviors and indicators of compromise</td>
</tr>
<tr>
<td>Automated, actionable technical guidance</td>
<td>- Support faster forensics and incident response</td>
</tr>
<tr>
<td>Robust reporting</td>
<td>- Support timely and more efficient compliance and audits</td>
</tr>
</tbody>
</table>

Source: Aberdeen, February 2021