REPORT: IS MAINFRAME SECURITY GETTING BETTER—OR FALLING BEHIND?

In spite of the longstanding perception that the mainframe is inherently secure, a full 91 percent of organizations with mainframes have experienced a compromise or breach of sensitive data in the last five years. For more than a quarter of organizations, it's happened between six and 25 times. That's according to *The Essential Holistic Security Strategy*, a recent report by Forrester Consulting, commissioned by BMC.

It's no surprise that hackers are finding their way into this critical enterprise system; today's connected mainframe is a long way from the isolated data centers of the past. And with the recent surge in work-from-home, its vulnerability has only increased. When it comes to mainframe security, there's clearly more work to do. But is it getting done?

The Forrester Consulting report, based on a survey of 310 companies, as well as interviews with security and mainframe decision-makers, examines the current state of mainframe security in the enterprise, how it has changed over the past year, and the characteristics of the most well-prepared organizations. Topics discussed in the report include:

- The strategies and priorities of security and mainframe decision-makers—and how they differ between "Ready" and "Not Ready" organizations
- Adoption trends and supporting technologies for Zero Trust
- Overcoming barriers to security and operations alignment to enable SecOps
- Recommendations for advancing mainframe security readiness

Ready or not

While many organizations are increasingly aware of the risks facing their mainframe environments, Forrester's analysis finds that over the past year, "companies overall have decreased their mainframe security readiness." In fact, while most teams realize that their data isn't safe, only 29 percent of survey respondents are taking steps to actively secure their mainframes—a decline of 12 percent from a year ago.

To gain insight into trends in security strategy optimization, Forrester categorized respondents according to their readiness to respond to mainframe-related security events. By comparing organizations in the "Ready" and "Not Ready" groups, the firm underscores the measures that define the most effective security teams. For example, "Not Ready" organizations tend to focus narrowly on detection, security monitoring, and threat intelligence, while "Ready" companies are taking a more holistic approach that includes building an internal culture of collaboration between security and operations teams, hiring additional IT security staff, and investing in mainframe security.

Extending Zero Trust to the mainframe

As companies move to close the mainframe security gap, many are emphasizing active security measures. Asked about their top security priorities over the coming year, 81 percent of survey respondents cited security orchestration automation and response (SOAR), while 76 percent named extended detection and response (XDR).

Zero Trust was considered a high or critical priority by 71 percent of respondents—and 84 percent of respondents agreed that it is important to include the mainframe in a holistic Zero Trust strategy.

Organizations that have already or plan to adopt a Zero Trust approach for their mainframe name benefits such as the ability to detect breaches, stop malware propagation within the mainframe, and prevent mainframe breaches.

Solving SecOps silos and friction

While Forrester underscores the importance of achieving alignment between mainframe and enterprise security teams, organizational barriers continue to impede progress on SecOps. More than half of respondents report friction between these teams, and a similar number find that their operations are too siloed to work together effectively. Addressing these challenges is high on the agenda for the coming year, with 81 percent of organizations prioritizing the integration of security functions and improving security detection and response. Both measures will help security and operations teams collaborate more successfully while also protecting the mainframe against active threats.

Forrester's analysis concludes with recommendations that advise mainframe and security leaders to:

- Work smarter—not harder—to reduce risk
- Hone their Zero Trust practices
- Bridge silos between security and operations teams
- Govern the mainframe as just another internet-connected device

To explore Forrester's findings in depth, download the full report, *The Essential Holistic Security Strategy: Mainframe Security Is Dangerously Absent From Enterprise Strategy*.