HOW BMC DEFENDS THE MAINFRAME FROM MODERN SECURITY THREATS

Enterprises Are Modernizing the Mainframe, but They Shouldn't Stop Short of Security

The experts who predicted the decline of the mainframe decades ago are still eating their words thanks to the platform's reliability and processing power at scale. Instead of becoming obsolete, mainframe reliance is on the rise, and Big Iron handles 68% of global production IT workloads, including 87% of the world's credit card transactions. However, while modernization of mainframe environments has improved their capabilities and kept them relevant long past the perceived expiration date, it's also added new security risks that enterprises must defend against.

Mainframe security has historically been taken for granted because accessing the mainframe used to require physical access and ability to use TSO/ISPF. Times have changed, and mainframes are now TCP/IP-connected computers that can be controlled from around the world (you can now find a 3270 emulator in the iPhone app store!). Because mainframes serve as the foundation for the financial, insurance, and healthcare industries, among others, they represent a treasure trove of sensitive data to cybercriminals.

The defense mechanisms used to protect your organization's other endpoints do little to defend the mainframe. Firewalls are unable to defend the multitude of network access points your employees

are carrying around in their pockets, and anti-virus systems primarily offer protection against established, documented threats on distributed systems.

Instead of these outdated defenses, your best practice for protecting your most valuable IT asset is to utilize a mainframe-specific security solution. With BMC's Automated Mainframe Intelligence (AMI) for Security, you gain access to these key defensive measures leveraging your current team of distributed cybersecurity professionals.

1. **Real-time reporting**
   The Ponemon Institute's 2019 Cost of a Data Breach report paints a grim picture of cybersecurity response times. It takes an average of 279 days for an organization to discover and contain a breach, which means criminals have more than nine months to steal your data and create backdoors so they can return whenever they want. It makes sense that a delayed discovery of a breach increases the cost of cleaning up the mess, but the magnitude is sobering. Breaches that take longer than 200 days to fix cost an average of $1.2 million more than those that are fixed within that time frame. AMI for Security includes an endpoint detection and response solution that provides real-time mainframe reports and automatically alerts security admins the moment a threat is detected.
2. **Powerful correlation capabilities**
   BMC's correlation engine turns your log data into events that can tell a story of potential threat for a more proactive approach to cyber threat. The software's advanced algorithms automatically spot and flag evidence indicating anomalous activity, ensuring you always know what's going on in your most important computing environments. Best of all, the algorithms can learn and improve over time, keeping your defenses up to date while allowing you to maintain an agile organization.
3. **Privileged user monitoring**
   Privileged users necessarily have open access to the mainframe, and if they want, they can cover their tracks by eliminating audit trails. If you have misgivings about that, you're not alone. A European study involving 500 IT decision-makers illustrated that just 9% felt safe from insider threats. In fact, a full 42% of respondents from the UK reported that privileged users were the company's primary source of cybersecurity risk. It's imperative to know what these users are doing with your most valuable IT asset, and AMI for Security ensures that no non-sanctioned action goes unaudited, and the privileged user will be none the wiser.

Mainframe security used to be a given, but those days are over. Mainframes will continue to serve the Global 500 into the distant future. They'll need to stand up to the slew of security threats that emerge daily. For a complete guide to insulating your organization's mainframe from growing cybersecurity threats, download our whitepaper titled "Mitigating Mainframe Security Risks with Endpoint Detection and Response." To learn more about AMI for Security, BMC's latest mainframe security product family, please visit bmc.com or reach out to an expert today.