3 STEPS TO SHORE UP YOUR MAINFRAME SECURITY WITH ENDPOINT DETECTION AND RESPONSE

For decades, mainframes were practically locked away like vaults, and it was easy to take their security for granted. Even if you could break into the room, you needed the expertise to know command lines to get what you wanted. With the advent of 3270 terminal emulators in the 1970s, mainframe functions could be controlled from a "PC" with the use of a coax adapter card, but you still needed vast mainframe programming knowledge to get what you were after. Now, thanks to the ready availability of emulator variants such as TN3270, special hardware is no longer required to tap into the mainframe. All you need is an internet connection. As a result, mainframe accesses have extended beyond what early mainframers could ever have imagined. Endpoint access has come a long way and you can now access a mainframe with an iPhone.

Today's mainframe is a TCP/IP-connected computer integrated with your enterprise, and new threats have emerged to test its penetrability. To ensure viable defenses against both internal and external threat, you should treat your mainframe like any other endpoint and implement an endpoint detection and response (EDR) solution. Here are the best practices to secure your most valuable endpoint:

1. **Security Operations Center (SOC) inclusion**
   Ponemon's 2019 Cost of a Data Breach report indicates a 4.9% year-over-year increase in the mean time to identify (MTTI) and mean time to contain (MTTC) a breach, putting them at 206 days and 73 days, respectively. This incredibly long lifecycle is inexcusable for the

regulated industries that rely on mainframes, and it's also expensive – a response time that lags over 200 days will end up increasing the overall cost by 37%.Security personnel can't stop what they can't see. To streamline identification and response, look for an EDR solution that offers complete integration with your enterprise SOC. In the case of AMI for Security, that means eliminating the mainframe and distributed personnel silos and allowing for a 360-degree real-time view of your security operations. Visit AMI for Security for more info on how we help the largest companies in the world do this.

1. **Security automation**
   Even adequately funded IT departments are facing a labor shortage because there simply aren't enough experienced professionals. In 2018, the U.S. Department of Commerce estimated there were 350,000 vacant cybersecurity positions in the U.S. alone, and Cybersecurity Ventures predicts 3.5 million unfilled positions globally by 2021.To accomplish more and maintain an agile team, EDR solutions must lean on automation. Automated triggers such as shutting down ports and admin alerts that are sent in real-time must be in play. AMI for Security amplifies the efforts of employees with pre-built intelligence that leverages industry leading mainframe penetration expertise to automatically monitor mainframe data accesses and provide real-time alerts against anomalous user/system behavior.

1. **Privileged user monitoring**
   With state-sponsored threat actors and high-profile breaches dominating the headlines, it's easy to pay a disproportionate amount of attention to external threats. On the other hand, just 9% of European IT decision-makers feel safe from internal threats. Whether from a malicious insider, a non-technical (careless) executive with privileged access, an infected employee device, or just a lost laptop, internal threats are everywhere.To ensure adequate protection across a vast number of endpoints, a solution like AMI for Security monitors users and tracks their individual actions, alerting administrators in cases of privilege escalation, rights violations, and anomalous login instances. Real-time surveillance for suspicious user activity empowers an immediate response to threats, allowing your organization to mitigate resulting damages or even avoid them entirely.

EDR is designed to provide advanced threat protection, but not all solutions are created equal.