



**CLEVER® Solutions Empowering Global Enterprises**

While the mainframe might be the most “securable” platform, it does not necessarily mean that mainframes are actively being secured. This is partly due to perceived security elsewhere in distributed systems and networks, and the wrong belief that mainframes are inherently secure.

There is no doubt that hacking and cybercrime are on the rise. In fact, it is estimated that most breaches go unnoticed for over 200 days at most companies<sup>1</sup>.

Like any other systems, mainframes are subject to ransomware attacks, cybersecurity threats and vulnerabilities that leave them open to serious exposures. Overlooking mainframe security is an industrywide issue today. Recent research shows that even though 85% of companies say that mainframe security is a top priority, 67% admit that they only sometimes or rarely make mainframe decisions based on security<sup>2</sup>.

Effective mainframe defense should include comprehensive measures that can detect early signs of an attack or an ongoing breach. Here are some key signs.

- Repeated failed password attempts
- Suspicious outbound traffic
- Unusual FTP or telnet activities
- Persistent port scanning
- Unexpected port usage

[AES](#) provides intelligent solutions that will make your mainframe network more secure. In order to detect unusual or suspicious network activities that could be data exfiltration traffic or hacker’s command-and-control infrastructure, you must first establish a comprehensive *baseline* to understand what the normal activity looks like. [CleverView® for TCP/IP](#) keeps track of detailed network activities on the application level, network protocol level, and network interface level, which all can be used to determine the baseline network traffic.

[CLEVERDetect for IDS](#) complements the z/OS Intrusion Detection Services (IDS) capabilities. It provides *FTP Server Logon Failure* analysis to identify potential attacks to the FTP server. It also serves as a repository of all IDS, SAF (System Authorization Facility) and subsystem security violation messages, and integrates them seamlessly into your existing Security Information and Event Management (SIEM) software.

**[Learn More About AES CLEVER Family of Products](#)**

[Free Trial](#)

[Webinar](#)

[Website](#)

[Email](#)