As companies scramble to advance their cybersecurity readiness with increased threats, many are adopting the “Never Trust, Always Verify” ***Zero Trust*** strategy to secure their organizations, in addition to the traditional perimeter-based security model.

Zero Trust is implemented by eliminating implicit trust while continuously validating every stage of a digital interaction. From the applications on the endpoints to the backend services running in containers or virtual machines, every access to the applications and data needs to be authenticated, authorized, and continuously validated for security configuration, whether they are in or outside the organization’s network.

To have a holistic Zero Trust strategy, mainframe security must be included if mainframes are part of your hybrid cloud infrastructure. While mainframes are highly securable, they are not inherently secure. AES can help you protect your most valuable assets, typically the client, transactional and institutional data on your mainframe.

CLEVERDetect® for IDS complements the z/OS Intrusion Detection Services (IDS) by detecting security events including unauthorized subsystem accesses, FTP server logon failures, SAF (Security Authorization Facility) violations, and alert messages from third-party security products. It can also share these mainframe security events with any enterprise SIEM (Security Information and Event Management) software providing real-time analysis and correlation of security alerts or offending network packets.

CleverView® for TCP/IP provides constant monitoring of your mainframe networks by establishing/refreshing the baseline workload, which can be used to detect unusual activities that could indicate data exfiltration due to security breaches.

Learn More About AES CLEVER Family of Products

Free Trial	Webinar	Website	Email