By implementing confidential computing, most enterprises hope to secure their data and assets to a half of these enterprises spend at least $100,000 per year preparing for audits. Furthermore, 98% of IT, security and engineering executives say their current methods for protecting data negatively impact productivity. The most popular methods companies are using to secure third-party data are secure access providers, and confirming they can't see into partner's/customers' encrypted data. To ensure malicious parties aren't accessing third-party data, most enterprises monitor access points and confirm to partners/customers that they can't see into encrypted data. Most enterprises are concerned about preventing cybercriminals from accessing third-party data and meeting legal mandates like GDPR. Given the vast amount of data in use from endpoint to cloud, and the mounting pressures on enterprises around the world. With rising cybersecurity concerns, a business's ability to innovate and grow is critical. confidential computing can enhance innovation. Confidential Computing: Protecting data from platform administrators and service providers, such as hypervisors. Prevent platform software (i.e. a platform hypervisor) from accessing data customer you can't see. Do you agree that securing exposures across the spectrum of access points would improve your engineering teams to innovate and suppliers? What are the top ways that data is most likely to be accessed by third-party systems? Which of the following projects/technologies do you monitor to protecting third-party data? How much would you estimate information security audit(s) costs your organization annually? More than one-quarter of organizations in the financial services industry face at least five audits annually. Manufacturers are the most likely to spend significant sums preparing for audits. How does your organization required to undertake every year? Nearly 100% of Enterprises are not Fully in Information Security Audits. Significant Numbers of IT Teams Invest in Manufacturing. Confidential Computing: Protecting data from platform administrators and service providers, or platform software, such as hypervisors. Prevent platform software from accessing data customer you can't see. Protect data from platform software, or platform software, such as hypervisors. Preparing for audits. Protect data from platform software, or platform software, such as hypervisors. Prevent platform software from accessing data customer you can't see. Do you agree it's critical that organizations invest in data protection to prepare for the implications/costs of Cyberattacks Network penetration? Do you agree that, if confidential computing can enhance innovation? How much does your current approach to securing third-party data? Do you agree that, if confidential computing can enhance innovation? Confidential Computing: Protecting data from platform administrators and service providers, or platform software, such as hypervisors. Prevent platform software from accessing data customer you can't see. Do you agree that, if confidential computing can enhance innovation? Confidential Computing: Protecting data from platform administrators and service providers, or platform software, such as hypervisors. Prevent platform software from accessing data customer you can't see. Do you agree that, if confidential computing can enhance innovation?