However, only 4% of respondents are completely confident in their current approach to securing that data. 96% of enterprise IT, security, and engineering executives agree that given the vast amount of data in use from endpoint to cloud, and the mounting pressures on third-party data today, what their confidence is in current security position when it comes to third-party data?

Nearly all enterprises represented in this survey undertake at least one security audit per year, with 62% of healthcare organizations saying productivity can be moderately impacted. When enterprises face five or more security audits per year, the impact on IT increases significantly.

Furthermore, 98% of IT, security and engineering executives say their current methods of securing third-party data are not sufficient, and they need new tools and zero trust architectures.

The most popular methods companies are using to secure third-party data are secure access management, data loss prevention, and data masking. These methods help to safeguard data when it is accessed by third parties.

To ensure malicious parties aren't accessing third-party data, most enterprises monitor access points and prevent platform software from accessing data. Confidential computing can enhance innovation and protect data from platform administrators and service providers.

A Pulse Survey on the Future of Security Technology

Confidential Computing: How Close to Reality?

Confidential computing is the ability to run applications on data without revealing the content to the underlying infrastructure. It is not yet a reality for most enterprises, as only 33% are currently using it.

When asked which of the following confidential computing security benefits would positively impact their organization the most, the majority of respondents chose prevention of platform software from accessing data.

Another benefit of confidential computing is protecting data from platform administrators and service providers, or platform software, such as hypervisors. This is seen as more important than preventing platform software from accessing data.

Prevent platform software from accessing data:

- 53%
- 27%
- 5%
- 2%
- 2%

Protect data from platform administrators and service providers:

- 53%
- 36%
- 12%
- 8%
- 8%

Protect data from platform software:

- 72%
- 47%
- 33%
- 31%
- 22%

According to our survey, 100% of manufacturers think securing exposures across third-party data is a high or top priority. This is a higher number than the survey-wide average (41%).

Financial services organizations (54%) are the most security-conscious sector by relative financial outlay. Further, 91% of enterprise executives believe confidential computing can enhance innovation.

Despite being ranked third, 41% of enterprises say securing confidential third-party data is a top priority. Confidential computing can be used to protect sensitive data from being exposed when interacting with third parties.

To ensure third-party data is secure, the majority of enterprises monitor access points and prevent platform software from accessing data. Confidential computing can enhance innovation and protect data from platform administrators and service providers.

A higher number of financial services organizations (54%) relative to the survey-wide average (41%), rank the protection of data from platform administrators and service providers as a top priority.

When asked which confidential computing security cases would be most impactful to your organization, the most important was preventing platform software from accessing data.

The top three most important types of data for confidentiality are payment information, personal information, and intellectual property. Confidential computing can be used to protect these types of sensitive data.

To ensure third-party data is secure, the majority of enterprises monitor access points and prevent platform software from accessing data. Confidential computing can enhance innovation and protect data from platform administrators and service providers.