Private Cloud Security in the Face of Ransomware Onslaught

Ransomware is an issue across the board. 68% have experienced ransomware in the past 24 months, with 37% of respondents reporting 3-6 attacks in that time.

Ransomware is a growing threat in the private cloud. In addition to attacks on their own organizations, 55% of respondents are aware of 3-6 peer organizations that have been attacked with ransomware at least once in the last 24 months (whether successful or not).

Where is your organization on the maturity of organizations protecting against ransomware with a Zero Trust architecture, most organizations do not have a robust plan in place and are left exposed and unprepared.

88% of respondents do not yet have a firm grasp on their Zero Trust plan & implementation.

87% of respondents are using at least 2 separate technologies. However, it's worth noting that 87% of respondents are using at least 2 separate technologies.

To maintain compliance, many organizations rely on multiple network security solutions. Despite not being industry standard, Next-generation firewall (NGFW) hardware and Windows firewall options are the most popular options. However, it's worth noting that 87% of respondents are using at least 2 separate technologies.

Additionally, tech leaders feel that network segmentation, micro-segmentation and IDS/IPS are the top 3 technologies to protect their organizations in the private cloud.

82% of respondents have at least one application that must comply with any of the regulations identified above. However, when it comes to protecting against ransomware in the private cloud, only 44% of respondents feel confident that their organization is protected.

74% of respondents do not feel ready to implement a Zero Trust plan.

Gartner Peer Insights and VMWare surveyed 200 IT decision makers.