Gartner Peer Insights. vmware

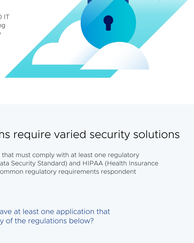
Private Cloud Security in the Face of Ransomware Onslaught

As ransomware attacks become an inevitability, protecting applications and workloads in the private cloud is more important than ever. However, when it comes to protecting against ransomware with a Zero Trust architecture, most organizations do not have a robust plan in place and are left exposed and unprepared.

Gartner Peer Insights and VMWare surveyed 200 IT and security leaders who are involved in managing networking or security to understand the security maturity of organizations' private cloud.

Data collection: February 20 – April 7, 2022

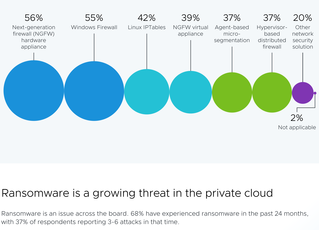
Respondents: 200 tech decision makers



Varied compliance regulations require varied security solutions

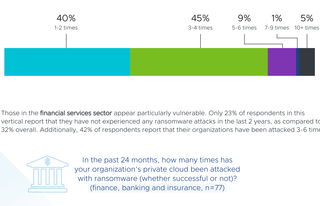
97% of respondents have at least one application that must comply with at least one regulatory requirement. PCI-DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Insurance Portability and Accountability Act) are the most common regulatory requirements respondent organizations must comply with.

Does your organization have at least one application that must comply with any of the regulations below?



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.

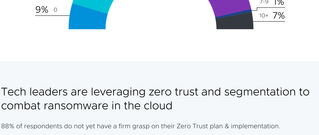
What network security technology do you use to comply with the regulatory requirements identified above?



Ransomware is a growing threat in the private cloud

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.

In the past 24 months, how many times has your organization's private cloud been attacked with ransomware (whether successful or not)?



Organizations that have been attacked in the past 24 months (n = 137)

Those in the **financial services sector** appear particularly vulnerable. Only 23% of respondents in this vertical report that they have not experienced any ransomware attacks in the last 2 years, as compared to 32% overall. Additionally, 42% of respondents report that their organizations have been attacked 3-6 times.

In the past 24 months, how many times has your organization's private cloud been attacked with ransomware (whether successful or not)? (finance, banking and insurance, n=77)

In addition to attacks on their own organizations, 55% of respondents are aware of 3-6 peer organizations who have suffered at least 1 ransomware attack in the last 24 months.

Roughly how many peer organizations are you aware of in your industry that have been attacked with ransomware at least once in the last 24 months (whether successful or not)?

Tech leaders are leveraging zero trust and segmentation to combat ransomware in the cloud

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

Where is your organization on its journey to enable Zero Trust for workload communications in the private cloud?

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

Please rank the following technologies to protect against ransomware in the private cloud from most to least relevant for your organization, with the most relevant on top.

Respondent Breakdown

Region

Title

Company Size

Gartner

Source: Gartner Peer Insights, Security in the Private Cloud survey