Gartner Peer Insights™ vmware®

Ransomware Incident Response

Ransomware attacks have become inevitable, but many organizations fail to plan ahead – leaving themselves overexposed and underprepared for an attack.

GPI and VMware surveyed 200 information security leaders who have experienced a ransomware incident in the last 3 years to understand how their organization responded and what they changed in the aftermath.

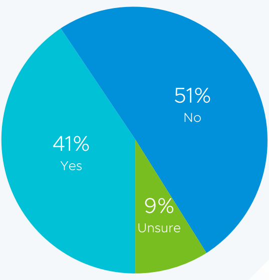
Data collection: June 8 - July 16, 2022

Respondents: 200 Infosec leaders

When ransoms are paid, they're often covered by insurance companies

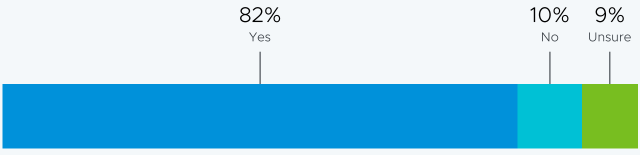
Among tech leaders who have experienced a ransomware incident in the last 36 months, over half (51%) said their company did not pay out a ransom.

Was a ransom paid out by the organization?



However, among those respondents whose companies did pay out the ransom (n=82), 82% say some or all of the ransom was covered by an insurance company

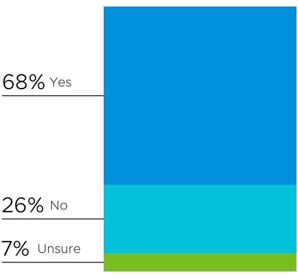
Was some or all the ransom covered by an insurance company? (n = 82)



Staffing is a key component of effective ransomware response and remains an issue for some organizations

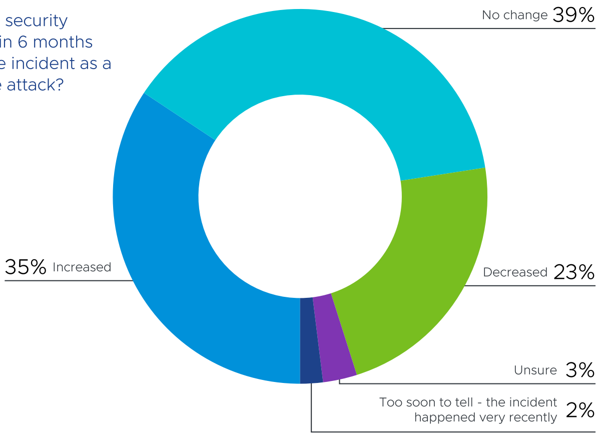
Just over two-thirds of respondents said that they felt their security team was adequately staffed at the time of the event.

In your view, at the time of the ransomware incident, was the security team adequately staffed?



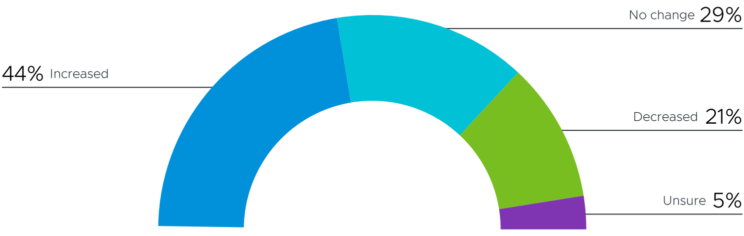
Overall, 39% of respondents say the size of their security team did not change within 6 months as a direct result of the attack.

Did the size of the security team change within 6 months of the ransomware incident as a direct result of the attack?



However, 44% of respondents who **did not** feel they were adequately staffed at the time of the attack (n=52) increased the size of their security team within 6 months as a direct result of the attack.

Did the size of the security team change within 6 months of the ransomware incident as a direct result of the attack?



Additionally, despite staffing increases only 40% of the of respondents who **did not** feel they were adequately staffed at the time of the attack feel that their team was adequately staffed 6 months after the attack.

Was the security team adequately staffed 6 months after the ransomware incident? (n=52)

40%
Yes

15%
Too soon to tell

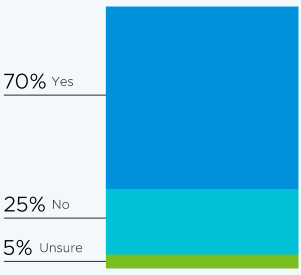
21%
No

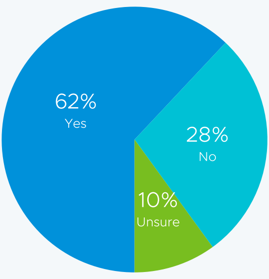
23%
Unsure

Incident response plans are effective and should be kept up to date

The majority of respondents (70%) say they had a ransomware incident response plan in place prior to their most recent ransomware incident occurred.

Was there a written incident response plan (applicable to ransomware) before the ransomware incident happened?



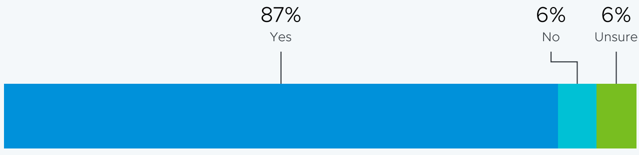


Additionally, nearly two-thirds (62%) of respondents who did not have a response plan in place say they created one after the incident occurred.

Has a written incident response plan been put in place since the ransomware incident occurred? (n = 60)

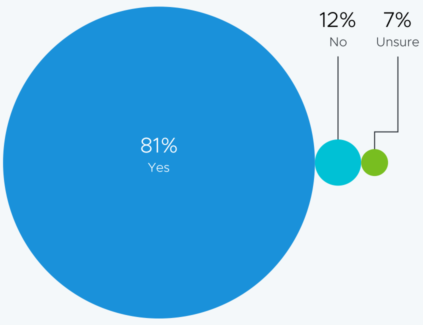
87% of respondents who had an incident response plan in place said the plan was followed.

Was the written incident response plan followed in response to the ransomware incident? (n = 140)



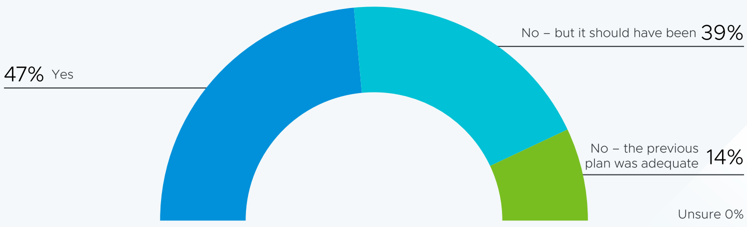
Among those who utilized an incident response plan, 81% said the plan was adequate or mostly adequate.

Was the written incident response plan adequate or mostly adequate to handle the ransomware incident? (n = 122)



Despite the efficacy of incident response plans, 47% of respondents updated theirs after their most recent incident. An additional 39% said that while their plan wasn't updated, it should have been.

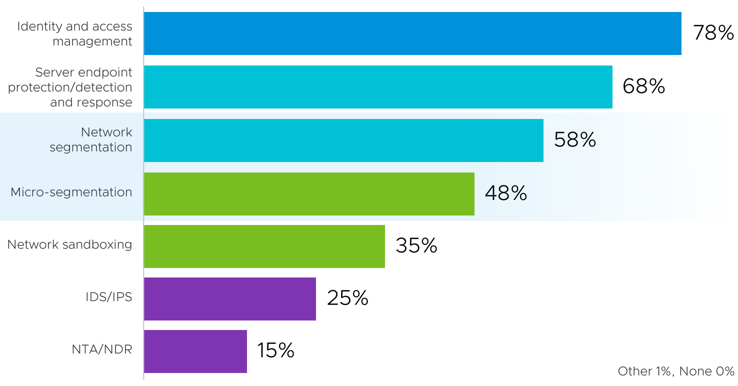
Was the written incident response plan updated after the ransomware incident? (n = 140)



Security leaders see promise in segmentation strategies to prevent ransomware incidents in the future

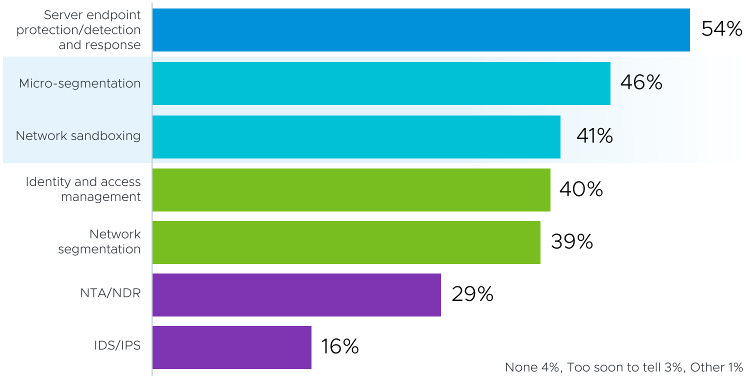
More than three-quarters of respondents had an Identity and access management solution in place prior to the ransomware incident.

Which of the following technologies did your organization have in place before the ransomware incident?



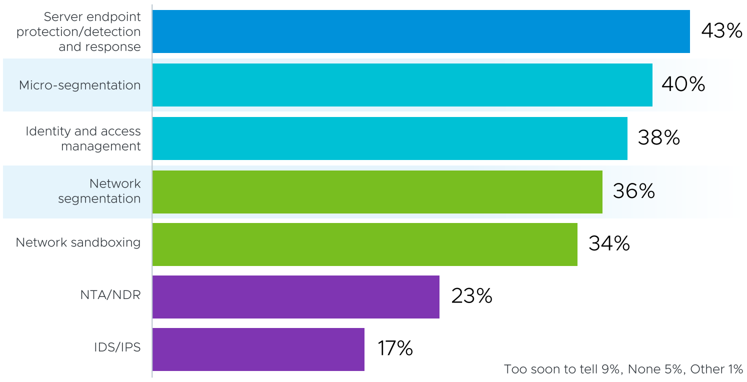
However, after the incident micro-segmentation (46%) and Network Sandboxing (41%) saw an increase in investment/deployment.

Which of these technologies saw an increase in investment/deployment after the ransomware incident?



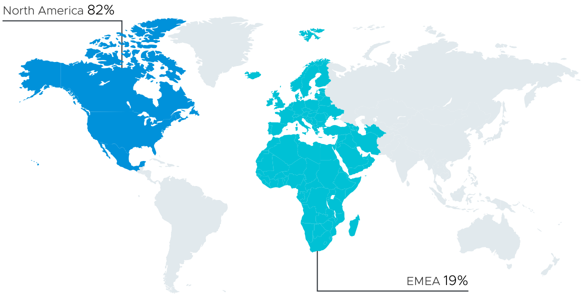
Additionally, 40% of respondents said micro-segmentation deserves a further increase in investment/deployment.

In your opinion, which of these technologies should see a further increase in investment/deployment?

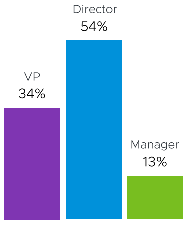


Respondent Breakdown

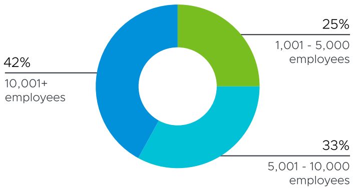
Region



Title



Company Size



Gartner

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, Ransomware Incident Response survey

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.