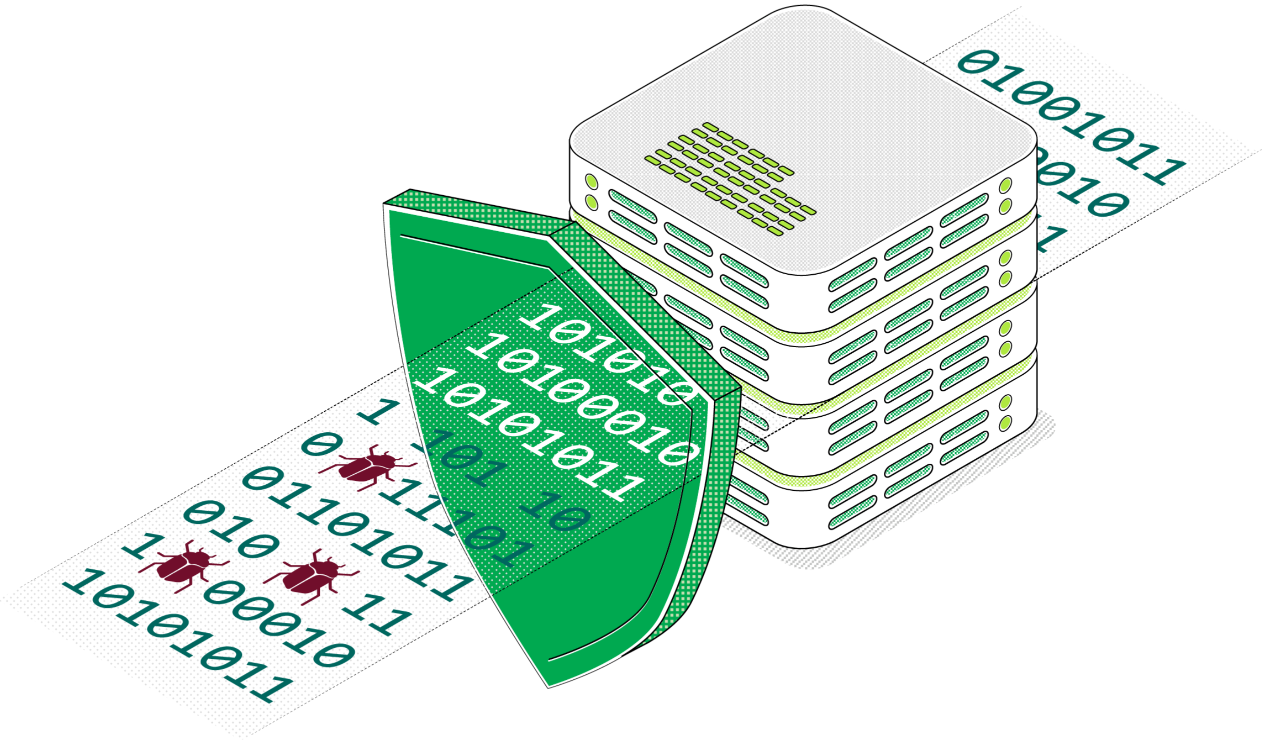
Veeam

# 2021 Ransomware Retrospective



# Introduction

Ransomware is one of the most serious and prevalent threats to modern data. When fundamental operations are disrupted, businesses find their hands tied and their capabilities lost to customers. According to a recent report from Cyber Security Ventures, an organization fell victim to ransomware every **14** seconds in 2019, and it's expected to be every **11** seconds in 2021. Ransome amounts have increased too. In mid-2018, the average ransomware payment was **$41,198**. By late-2019, that price more than doubled to **$84,166**.

In 2020, Veeam® participated in research to understand ransomware's impact on the global IT community and its customers. From June – August 2020, data from **over 1,700** respondents was recorded across nine major business sectors. All customer segments were represented including **39%** from organizations with under **250** employees, **43%** between **250** and **2500** and **18%** over **2500**. EMEA made up the bulk of the respondents with **42%**, North American **33%**, LATAM **10%**, APJ **10%** and MEA **5%**.

Veeam believes that the best offense is a solid defense. To improve your defenses, it's essential to understand how cyber threats have evolved and ensure you have a robust strategy for recovering from an attack

This white paper will help you understand how threats have changed the way we conduct business and provide a benchmark for the effectiveness of defenses with the goal of preventing considerable downtime, data loss and paying a costly ransom.

# Key findings

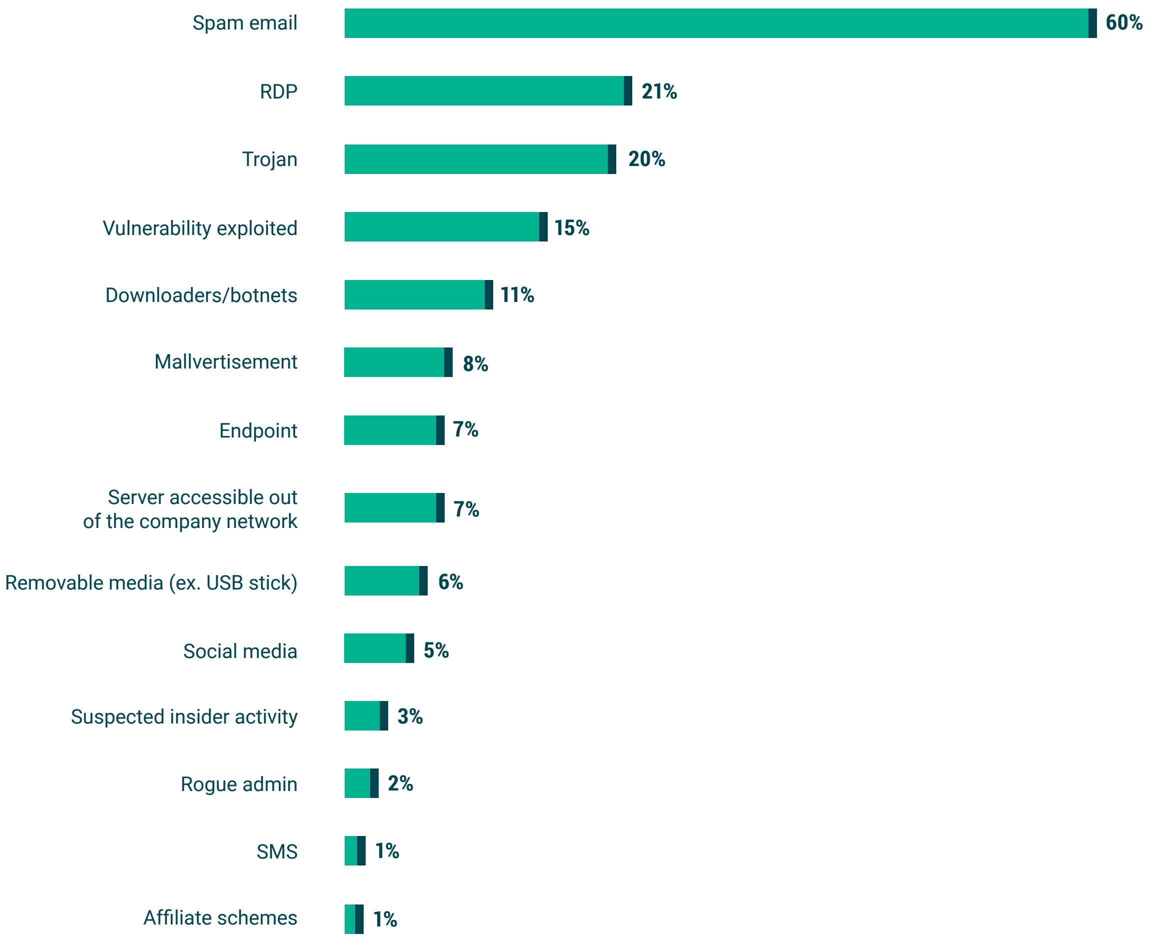
- The business impacts from ransomware attacks have been getting better in terms of data loss (**25%** vs. **33%** in 2018), downtime (**24%** vs. **41%** in 2018) and loss of productivity (**21%** vs. **28%** in 2018).
- Increase in the top ransomware infection source from spam email (**60%** vs. **48%** in 2018), mostly with single or multiple endpoint devices (**57%** globally).
- **71%** of global respondents who were infected were able to recover **91%** or more affected data.
- Mitigating ransomware attacks were handled more often by end-user education (**20%**), bolstering backup storage resiliency (**19%**) and securing internet access (**16%**) globally.
- Many Veeam customers have implemented offline air-gapped or immutable backups with hardware storage (**51%**).
- The majority (**92%**) of global Veeam customers had zero financial impact due to data restore, lost productivity or lost sales due to ransomware-inflicted downtime.

## Ransomware attack infection source

Spam email is by far the most frequent infection source (**60%** compared to **48%** in 2018), with remote desktop protocol (RDP) (**21%**) a far-off second and Trojan attacks (**20%**) the third most common. Regionally, RDP was rated higher in the Middle East and Africa, Latin America and Asia. By segment, after spam and RDP, downloaders/botnets come in third, especially for companies with **5,001–10K** employees. Large enterprise noted impact from vulnerability exploited and suspected insider activity.

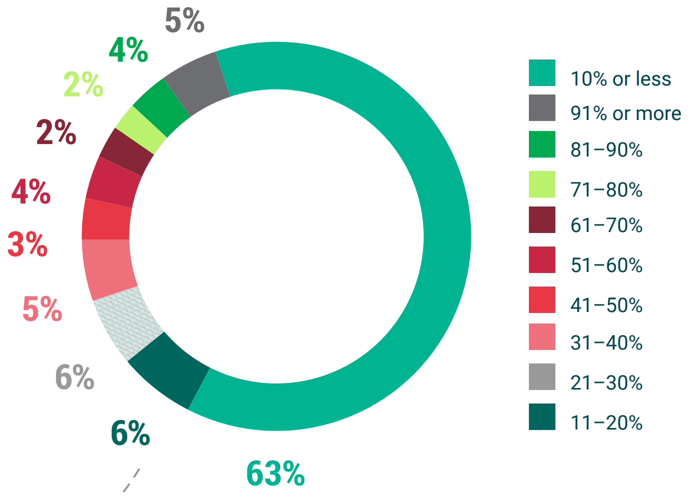
SPAM email and RDP remain the #1 and #2 most prevalent ransomware vehicles. While this can be mitigated, somewhat, with education, it shows that both detection, response and recovery plans need to continue since we cannot always trust the end-user practices.

What was the ransomware infection source? Check all that apply.



## Percentage of data encrypted by attack type

Globally, the majority of respondents indicated that **10%** or less of production data was encrypted by a ransomware attack. However, two demographics indicated ransomware encrypted a much higher percentage of their production data compared to the rest of the world. Ransomware hit both enterprises with **+100K** employees, and respondents in the Middle East and Africa extremely hard, with **91%** or more of their production data compromised. However, even though **63%** of respondents showed less than **10%** of their data was attacked, there is no choosing what type of data was targeted, see below. Encryption tends to target the most used data, replication and backups.

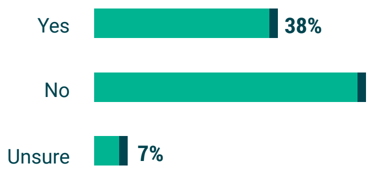


For the most recent incident, what percentage of your production data do you estimate that the ransomware attack successfully encrypted?

## High-priority data encrypted

When asked about the importance of the data affected by ransomware, **38%** of respondents indicated that "high-priority" data was encrypted as part of an attack. Asia doubled this response at **63%** compared to the global and individual region results. Larger enterprises of **+100K** employees and SMBs noted a similar trend at **67%** and **54%**, respectively.

This again showcases that data critical for organization operations and success is left vulnerable to attack. While ransomware often does not discriminate, working it's way through systems and data stores, the data organizations value to the most is inevitably touched.



Did the ransomware attack encrypt any data that is perceived as «high-priority»?

## Primary outcomes of ransomware attack

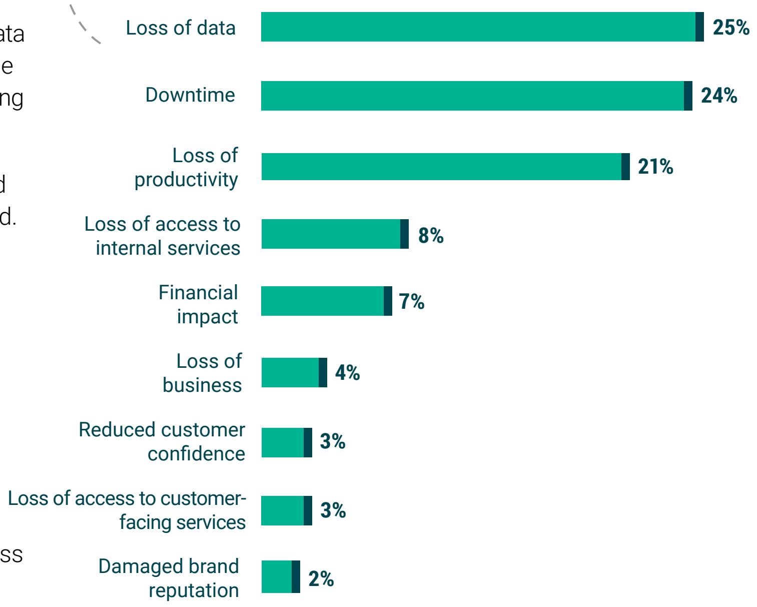
The primary negative effects on business from attacks were data loss, downtime and productivity. In APJ, MEA and NA, downtime was more often the outcome. Loss of access to customer-facing services was the #1 response for large enterprises.

The data also provided some positive news. When compared to our previous study, several key negative outcomes dropped.

| Attack outcome | 2018 | 2020 | % Change '18 to'20 |
|---|---|---|---|
| Data loss | 33% | 25% | ↓ 8% |
| Downtime | 41% | 24% | ↓ 17% |
| Productivity | 28% | 21% | ↓ 7% |

Usually, organizations focus on the immediate cost of ransomware attacks — downtime and data loss. But deeper impacts are often felt after the initial attack, including loss of access to internal services, negative financial impacts and loss of business.

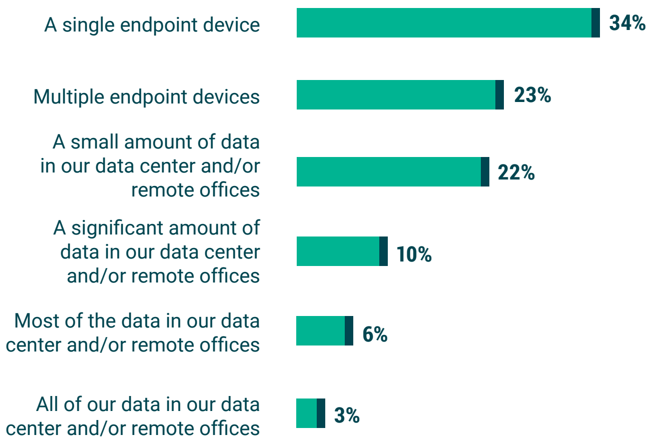
What were the main outcomes of the attack? Check all that apply.



## Ransomware infection

Over a third of customers were infected from a single endpoint device, consistent at the region and segment levels. The only exceptions are for Australian and New Zealand and commercial to small enterprise customers who experienced a small amount of data loss in their data center and/or remote offices.

With the increase in remote endpoints connected to business data and system in 2020 due to the global pandemic, there was a massive spike in ransomware exploiting these endpoints. And due to remote collaboration, it was quickly shared and disseminated between users.

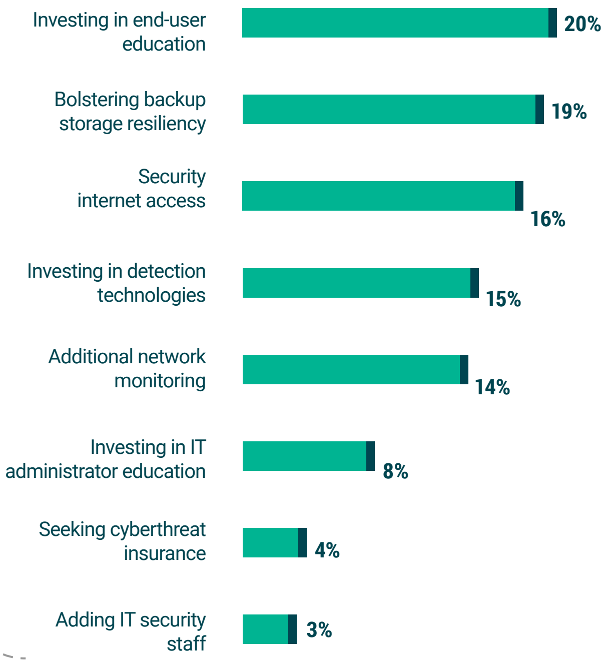


How widespread was the ransomware infection? Check all that apply.

## Mitigating ransomware attacks

End-user education (**20%**), bolstering backup storage resiliency (**19%**) and securing internet access (**16%**) are the top choices of ransomware mitigation globally. Similar results are seen from a geo perspective where NA, LATAM and EMEA/MEA are more apt to invest in detection, while NA was more likely to use additional network monitoring for mitigation.

To better mitigate ransomware vulnerabilities, customers are now focused on bolstering backup storage resiliency, through immutability, investing in end-user education and securing internet access.



What steps are you taking to mitigate a potential ransomware attack in the future? (Check all that apply)

# The Veeam impact

Veeam believes that the best offense is a solid defense, including having a robust strategy for backing up your data. The results of this study show improvement in the ability to detect, respond and recover from a ransomware attack but there is still significant work to be done. Over the course of this study, we found a large majority (**92%**) of Veeam customers had no financial impact due to data restore, lost productivity or lost sales due to ransomware-inflicted downtime. Almost a quarter of Veeam customers experienced a financial loss of less than **$25K** when ransomware hit.

As any downtime means lost revenue, Veeam customers had mechanisms to recover fast when implementing effective ransomware solutions. We see this in the case with over **60%** of the customers surveyed who experienced no financial impact due to their ability to quickly recover from ransomware attacks.

Successful backups are the last line of defense for cyberattacks and can be the deciding factor to prevent considerable downtime, data loss and paying a costly ransom. Veeam offers actionable strategies, rotating backup copies across several locations and leveraging cloud options to make your backups practically immutable.

To help measure the effectiveness of your defenses, Veeam has an easy 12-question gap assessment to identify areas of improvement. You can then download the Ransomware Preparation Kit to get started building a more robust security program for the future.

**85%**

of Veeam customers cut their average ransomware recovery costs **under $25K**

**92%**

of Veeam customers have to spend **NOTHING AT ALL**

Assess your ransomware threat

Download the Ransomware Preparation Kit

## Sources

Steve Morgan, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, Cybercrime Magazine, October 2019

Coveware, Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate, Report on Q4 2019

Veeam Ransomware Customer Study, 2018 and 2020

veeam.com