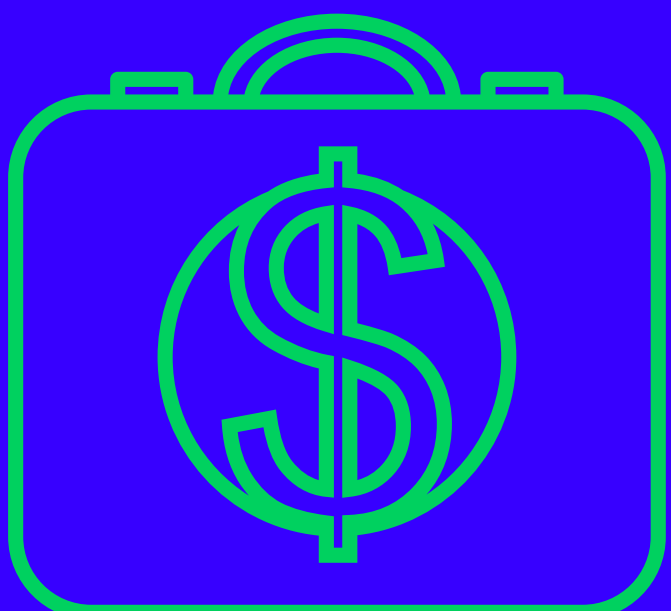


# Ransomware attacks are escalating.

According to Veeam's 2024 Ransomware Trends report, it was found that...



75%

of organizations have been hit by ransomware at least once in 2023.

Bad actors will now target your backup.

96%

of attacks targeted backups and

76%

were successful.

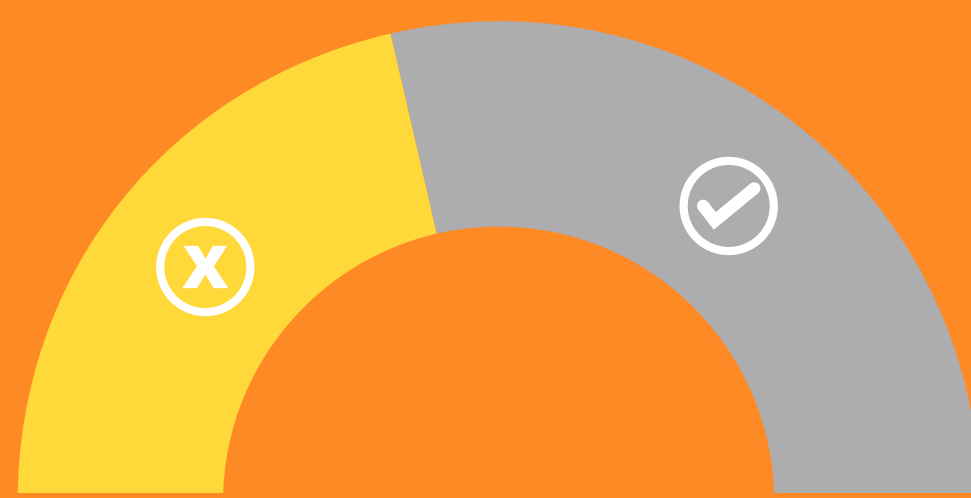


Paying ransom ≠ solution

The ransom is only

32%

of the financial impact organizations will experience.



43% of affected data won't be recoverable.



## Where does Singapore stand?

Singapore's national position is that payment of ransoms to attackers is strongly discouraged. In Counter-Ransomware Task Force (CRTF)'s report, it is recommended that we focus on 4 pillars of actions.

### Pillar 1:

Strengthen defences of high-risk targets so successful attacks are harder to launch.

### Pillar 2:

Disrupt ransomware business model to reduce the pay-off.

### Pillar 3:

Support recovery so victims don't pay ransom, which fuels ransomware industry.

### Pillar 4:

Work with international partners to ensure a coordinated global approach.

## Fortifying Against Ransomware: Veeam's Alignment with CRTF Strategies

### Prevent Attacks



Application Control



Patch Applications



Configure Microsoft Office Macro Settings



Application Hardening

### Limit Impact of Cyber Attacks



Restrict Admin Access



Patch Operating System Vulnerabilities



Implement Multi Factor Authentication

### Data Recovery and System Availability



Daily Backups

Download the full whitepaper: [Comprehensive Ransomware Mitigation Strategies for Singapore](#)