veeam

A Gartner® Magic Quadrant™ Leader seven times running*

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 Malaysia stand?

Malaysia's new Cyber Security Act emphasises prevention, urging agencies to implement multi-layered security measures, with backups as crucial defense. The 4 key requirements of the Act are:

Act 1

Provide information on critical infrastructure.

Act 2

Implement code of practice.

Act 3

Conduct cyber security risk assessment and audit.

Act 4

Give notification on cyber security incident.

Malaysia's cybersecurity authorities advise companies hit by ransomware to refuse paying cyber criminals and seek assistance from the Cyber999 service, filing reports online.

Fortifying Against Ransomware: Veeam's Alignment with Malaysian Cyber Security Act 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 Malaysia

*Gartner, Magic Quadrant for Enterprise Backup and Recovery Software Solutions, Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham, 7 August 2023.