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 India stand?

India's national stance emphasizes the importance of not paying ransoms to cybercriminals, aligning with a coalition of 50 nations dedicated to disrupting the ransomware payment ecosystem. According to Cert-In's ransomware report, organizations are urged to follow a four-step response protocol:

Step 1:

Disconnect infected systems,

Step 2:

Determine the scope of infection,

Step 3:

Identify the ransomware strain,

Step 4:

Work with international partners to ensure a coordinated global approach.

Fortifying Against Ransomware: Veeam's Alignment with Cert-In 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 India

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