

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.

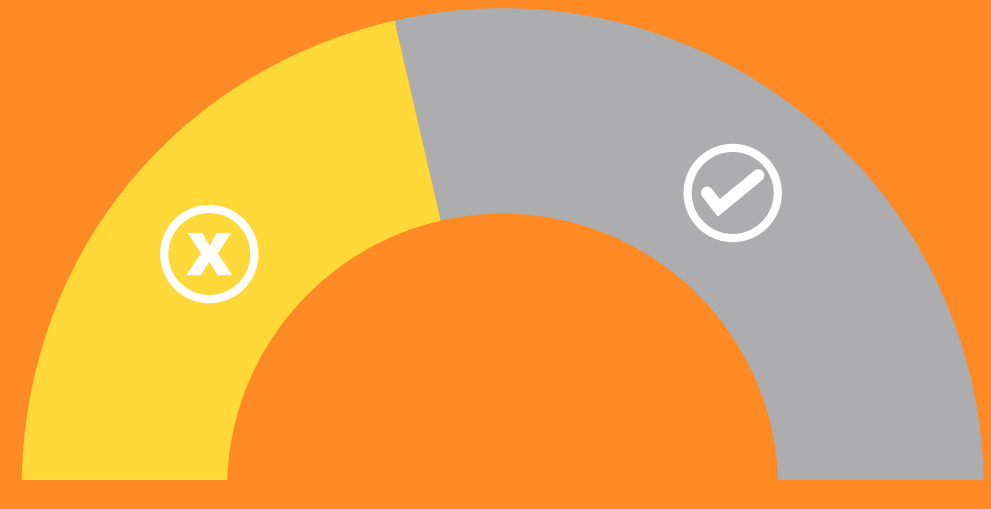
Bad actors will now target your backup.

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 Indonesia stand?

Indonesia has several regulations and guidelines to address the mounting security threats that the country has faced in recent years, such as:

-  Regulations for national security and crisis management.
-  Cybersecurity for financial individual.
-  Personal data protection.

Fortifying Against Ransomware: Veeam's Alignment with Indonesian cybersecurity regulations

- 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

According to IDC's most recent Semiannual Software Tracker for Data Replication & Protection software, Veeam is #1 Worldwide for market share. Download the full whitepaper: [Comprehensive Ransomware Mitigation Strategies for Indonesia](#)