Why isn't backup and recovery enough to handle ransomware?

Short answer: Backups address only the final stage of a ransomware attack — encryption. By the time encryption starts, attackers have usually already stolen credentials and exfiltrated your data. Restoring from backup recovers your files; it does nothing about the data already in the attacker's hands.

Ransomware is the last step, not the first

A typical intrusion runs in three stages:

1. **Identity theft** — credentials are compromised to gain access.
2. **Data theft** — intellectual property, customer records, and other sensitive data are exfiltrated.
3. **Encryption** — files are locked and a ransom is demanded.

Recovery strategies engage only at stage three. The confidentiality breach and loss of operational control have already happened.

The real cost

The largest business risk from ransomware usually isn't the ransom itself — it's revenue lost to a prolonged outage and the reputational damage that follows. Preventing the initial compromise protects both, which is why prevention has to come before recovery planning rather than instead of it.

Revision #3
Created 2026-07-20 19:23:44 UTC by Dennis Underwood
Updated 2026-07-21 19:32:00 UTC by Dennis Underwood