IBM Storage

Ransomware
Are you protected?

Real Impacts

This is the recent experience from a UK retailer:

46 Days to recover online retail business, other systems took months

$**400M** in lost profits

$**1BN** wiped off market value in the first week

When the attack comes, will you be prepared?

The Risk

Every year 63% of clients will be hit by Ransomware. Over 3 years that's a 95% chance, no longer a probability but a certainty.

Not IF, but WHEN you will be hit.

No Protection

75%

My security will keep them out!

75% of attacks entered through and open door either with real credentials obtained from phishing, theft or disgruntled employees or by system/human error

94%

I can recover from my back up.

94% of organisations attacked say their backups where targeted, removing recovery options and forcing ransom payment

40%

I'll pay the ransom.

40% of those who paid still did not get all their data back, some found that payment was illegal

76%

Somehow, I'll recover my business quickly.

76% of businesses take more than 100 days to recover.

IBM

The IBM Operational Resiliency Solution

Immutable, quantum encrypted **Protection**

Drive-level threat **Detection** in under 60 seconds

60 second **Recovery** guaranteed

Protect against ransomware and secure clean recovery points:

Traditional data protection often falls short replication can spread corruption, and backups are targeted in 57% of attacks, making recovery impossible.

With IBM FlashSystem immutability: Safeguarded Snapshots are logically air-gapped for clean, reliable recovery.

Quantum-safe encryption: FlashCore Module 4 (FCM4) reduces data loss risk and supports certified data deletion.

Application-aware recovery: IBM Storage Sentinel enables faster, smarter recovery points.

Detect threats to your data and systems:

Early threat detection is key to reducing financial and operational impact.

With IBM FlashCore Module 4: Analyze ransomware activity at the I/O level with real-time stats, **delivered in just 60 seconds.**

Using cloud-based AI: IBM Insights PRO threat detection engine is trained on known ransomware behaviors.

Live monitoring: IBM Defender sensors monitor server activity to detect active threats

Snapshot integrity checks: IBM Sentinel indexes data to scan for vulnerabilities and ensure SafeGuarded Copy snapshots are safe to recover from.

Recover and reduce downtime after a ransomware attack:

Aim for the lowest possible RTO and ensure systems are restored at full performance not slowed down by sub-optimal backup infrastructure.

Leverage faster recoveries: Access clean, uncorrupted backups from air-gapped snapshots, restored almost instantly at native Flash speeds.

Exploit SafeGuarded Copies: Restore **within 60 seconds** after an attack, preserving forensic evidence and delivering production-level performance.

Automate application recovery to reduce mitigation time with rapid, trusted snapshot restores

Take the Cyber Resiliency Assessment today

IBM