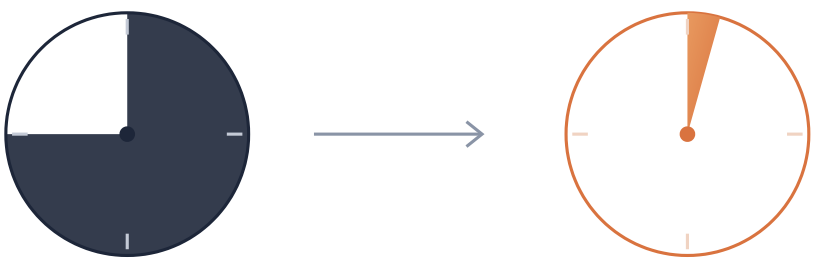
core6

AI has collapsed the time from disclosure to exploit

Defenders used to have weeks between a vulnerability being disclosed and attackers weaponizing it. AI-assisted tooling compresses discovery, exploit development and delivery into a fraction of that time — and storage & backup systems are the prize.



Before AI
Days to weeks to exploit

With AI
Seconds to exploit

Every stage, accelerated

AI automates the work that once needed a skilled human and a lot of time.

Initial compromise → Discovery → Exploitation → Lateral movement

The IT control plane is the new perimeter

Perimeter defenses can no longer protect everything. Storage and backup are on the new perimeter — prime targets and the last line of recovery.

- Storage & backup systems hold the data attackers want to encrypt, steal or destroy.
- They sit outside the view of EDR, vulnerability scanners and CSPM.
- A single misconfiguration can expose both production data and its backup infrastructure.
- Compromising the backup removes the victim's ability to recover.

Shrink the exploitation window on Storage and Backup

When attacks move at machine speed, defense has to be continuous, not periodic.

BEFORE A PATCH EXISTS

Continuous hardening

Keep every storage and backup system locked to a hardened baseline, so exposures attackers rely on are already closed — the best defense while no patch is available.

ONCE A PATCH EXISTS

Fast remediation

Detect drift and missing patches immediately and fix fast — with StorageGuard's "Fix It" auto-remediation — collapsing the window attackers have to act.

Close the window before AI finds it

Get a tailored analysis of the security posture across your multi-vendor storage and backup environment.

Talk to an expert

Dell · NetApp · Hitachi Vantara · Everpure · Infinidat · VAST Data · HPE · IBM · Huawei · Cisco · Broadcom · Nasuni · CTERA · Cloudian · Oracle · Veeam · Cohesity · Rubrik · Commvault

© 2026 Core6 Cybersecurity