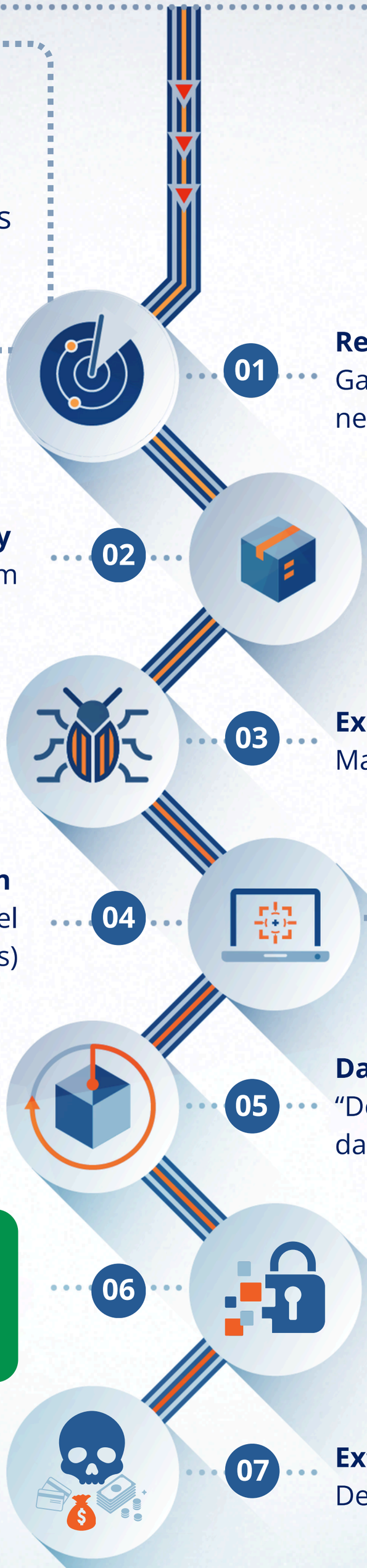
CERTES DPRM:
BREAKING THE *KILL CHAIN.*

How Certes Data Protection & Risk Mitigation (DPRM) prevents Active Directory breaches before they happen: By breaking the kill chain, we can stop attacks in their tracks – protecting the data rather than relying solely on network-based defenses.

How does DPRM break the kill chain?

- Preventing Escalated Privileges
- Mitigating Data Exfiltration
- Quantum-grade encryption



01 Recon
Gather intelligence about a target network

02 Delivery
Malware sent to target system

03 Exploitation
Malware executed on target system

04 Privilege Escalation
Gains full control with admin-level privileges (gaining admin rights)

This is where traditional perimeter security fails to protect your data, leaving you exposed

& where DPRM's proactive approach succeeds in protecting your data, keeping you safe

05 Data Exfiltration
"Double Extortion" Steal sensitive data before encrypting local copy

DPRM stops the extortion and ransomware demand by making the data useless to the attacker, devaluing it and giving them nothing to use against the target company

06 Encryption
Render data inaccessible to the victim

07 Extortion & Ransom Demand
Demand payment to restore access

The Result:
The kill chain is broken at the most critical stage, preventing ransomware from spreading and stopping data exfiltration before it even starts.