

The exposure window: why **continuous hardening** is the defense before the patch

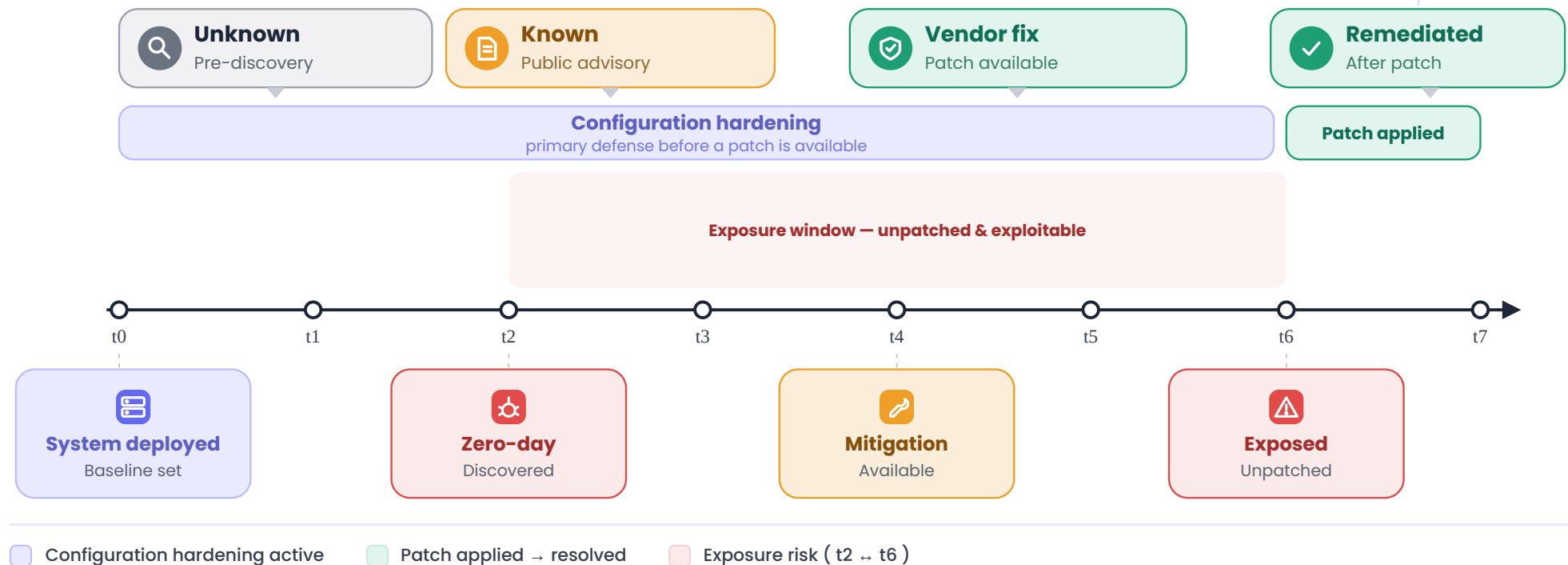
AI has accelerated **every stage** of the attack

The **IT control plane** is the new perimeter

Storage & backup systems are prime targets

The vulnerability lifecycle — and where the risk lives

[EXPOSURE WINDOW / ILLUSTRATIVE]



Before a patch exists: continuous hardening

Claude Mythos Preview uncovered thousands of zero-day vulnerabilities across major operating systems. Until a fix ships, continuous configuration hardening is the best defense against exploitation — closing the doors an attacker would use.



Once a patch exists: fast remediation

When a vendor fix becomes available, speed is everything. Fast, validated remediation collapses the exposure window — the stretch of time between a weakness becoming known and it being fixed, where attackers do their work.