Cyemptive

CYEMPTIVE PERIMETER FORTRESS [CPF]

The Firewall Was Never a Fortress

Even today's best AI-enabled firewalls still have to detect an attack (sometimes mulitple times) before they can learn to counter it. **By then, it's too late...**

Zero-day exploits slip through, admin credentials get compromised, policies get altered and persistence takes hold.

If detection-based perimeter security worked, attackers wouldn't live inside networks for months. **So why keep reinforcing the same model?**

Redefining Perimeter Security

x The Detection Model

- Detect → Block → Recover
- Signature dependent
- Persistent runtime
- Manual policy recovery
- Reactive containment

✓ The CPF Model

- **Detection-independent enforcement**
- **Controlled runtime lifespan**
- **Continuous configuration validation**
- **Autonomous restoration**
- **Structural containment**

Introducing Cyemptive Perimeter Fortress

CPF enforces structural perimeter resilience across enterprise trust boundaries. It limits persistence, validates integrity, and restores autonomously, without relying solely on detection.

LAYERED ENFORCEMENT ACROSS ARCHITECTURAL TRUST BOUNDARIES

Internet Edge	Enterprise Core	Office Zones	Data Center Segmentation	Command & Control Isolation

Preempt First. Detect Later. Operate Continuously.