

CYEMPTIVE PERIMETER FORTRESS [CPF]

The Firewall Was Never a Fortress

Even today's best AI-enabled firewalls still have to detect an attack (sometimes multiple times) before they 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 re-inforcing the same model?*



Redefining Perimeter Security



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 rejects persistence, validates integrity, and restores autonomously, without relying on detection or behavioral heuristics. It's the Ideal Zero Day solution for OT and critical infrastructure networks where lives and fortunes rely on faultless system integrity and availability.

Layered enforcement across architectural trust boundaries:

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

Preempt First. Detect Later. Operate Continuously.

CYEMPTIVE PERIMETER FORTRESS [CPF]

Extending Perimeter Fortress to Operational Technology (OT)

OT environments (such as industrial control systems, SCADA networks, utilities, manufacturing, transportation, and healthcare operations) operate under different security constraints than traditional IT networks.

Many of these systems are legacy platforms designed for safety and availability, not modern cybersecurity. They are often difficult or impossible to patch, cannot run security agents, and rely on protocols that lack authentication or encryption.

As OT systems become connected to enterprise networks and cloud infrastructure, traditional detection-based security models struggle to protect them.

Common challenges include:

- Security agents cannot run on many OT devices.
- Downtime for patching or recovery is unacceptable.
- Legacy protocols lack built-in security.
- Detection tools often generate excessive false positives.
- Incident response can disrupt critical operations.

These conditions allow attackers who compromise enterprise networks to move laterally toward operational environments and maintain persistence.

CPF for OT Environments

CPF protects operational environments by enforcing structural integrity at the infrastructure boundaries surrounding OT systems, rather than relying on detection inside fragile devices.

CPF continuously validates and restores trusted configurations across IT–OT trust boundaries while preserving operational stability. **CPF enables:**

- Continuous validation of segmentation policies.
- Autonomous restoration of trusted configurations.
- Structural containment of lateral movement.
- Isolation of command-and-control paths.
- Protection of legacy operational systems without modification.

What This Means for Critical Infrastructure Operators

With Cyemptive Perimeter Fortress:

Operational continuity improves

Industrial processes remain stable even when enterprise networks are targeted.

Legacy OT systems remain protected

Security does not require modifying fragile equipment.

Attacker persistence is minimized

Threat actors cannot maintain long-term control of operational network segments.

Recovery time is reduced

Trusted configurations are restored automatically.

Securing the Convergence of IT and OT

As enterprises connect operational systems to enterprise networks and cloud environments, the attack surface expands dramatically. CPF provides a pre-emptive structural defence layer that protects both enterprise and operational infrastructure.

Preempt First. Detect Later. Operate Continuously.

Cyemptive Technologies: Pre-emptive Cyber Defence by Design