

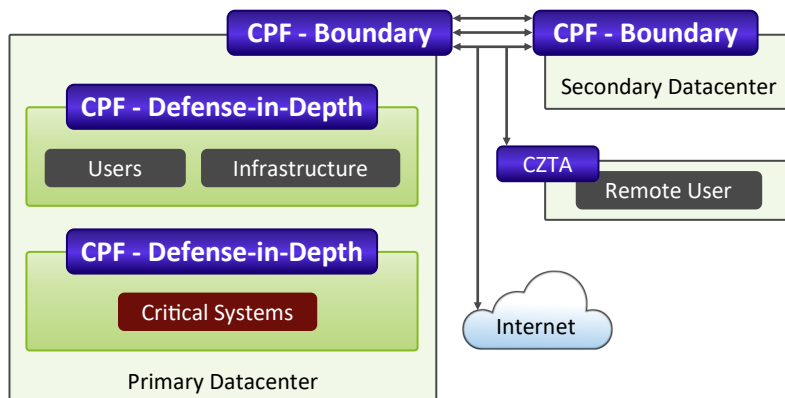
What is CPF?

The **CPF** is a highly available revolutionary perimeter defense solution for datacenters which stops today's most advanced global hackers and provides security at load balancer, proxy server, and web server levels. It does this in seconds and prior to compromise. CPF prevents network, root level and firmware attacks with ease as our patented underlying CyberSlice® technology does not wait for a compromise to occur. It's the only solution that prevents Zero-Day attacks both Discovered and Undiscovered as well as persistent advanced attacks, AI offensive and today's quantum computing attacks. CPF supports Cyemptive Zero Trust Access (CZTA) for secure, encrypted clients to replace compromised and vulnerable VPNs.

The Problem

Today's firewall and perimeter solutions are not stopping advanced global hackers or preventing new sophisticated, persistent threats. They don't properly protect network perimeters, stop AI offensive threats or quantum computer attacks, handle all root level firmware, Zero Day attacks, nor provide the ability to withstand and thwart attacks in seconds. Leading vendors don't have the confidence to offer financially backed SLAs in Seconds/Minutes. **Why let an attacker into the network to attempt to find them later?**

Multiple Perimeters for Defense-in-Depth



CPF - Boundary mode, prevents North-South attack vectors and secures boundary access into datacenters and communications between datacenters using IPSec, encryption, and Cyemptive's patented CyberSlice® technology. Supports CZTA for remote users.

CPF - Defense-in-Depth mode creates secure, Zero Trust internal perimeters to prevent East-West mobility, Data Exfiltration, and eliminate Insider Threats securing users, infrastructure, critical systems. Use as many as needed to create multiple perimeters.

**SECONDS-BASED
RESPONSE**

**PERFORMANCE
GUARANTEES**

**PREVENTS
ZERO-DAY
ATTACKS**

Consider This: All organizations being compromised are using the same Vendors, Hardware, Software, and Technologies! They are just NOT working, and NOT working together as a complete solution.

THE CYEMPTIVE DIFFERENCE

- **Cyemptive** has developed **revolutionary, patented technologies, Zero Trust Blueprints (ZTBs)**, and solutions to detect and pre-emptively stop attackers before they can infiltrate networks achieving new cyber-standards unlike any seen.
- **Cyemptive detected and successfully defeated over 540+ zero day attacks** in 2019-2020 alone. Our Zero Trust integrated protection platform prevents the most elite hackers from compromising perimeter defenses.
- **Cyemptive** won the DHS Border Security Technology Consortium (BSTC) Award for **most innovative technology**.
- **Cyemptive** is the first company to offer the industry Cyber Service Level Agreement (CyberSLA) performance measures providing new, **unprecedented, financially backed, seconds-based performance guarantees** for our customers.

RANGE OF SOLUTIONS

- CPF-1000 Boundary (datacenter, high-availability)
- CPF-1000 Defense-in-Depth (datacenter, high-availability)
- CPF-505 Boundary (SOHO, single or pair)

Jun 2021