

CYEMPTIVE TECHNOLOGIES:

The Industry leader in pre-emptive cyber defence

A Disruptive Approach to Cyber
Enterprise-Scalable Solutions
Risk Reduction, Resilience & ROI
Incident Response Process



October 2025

What Makes Cyemptive Unique?

Cyemptive Technologies is a pre-emptive cybersecurity platform, that goes beyond traditional reactive and proactive models. To avoid the high false-positive and false-negatives associated with predictive models, we have taken End-to-End Zero Trust to the logical extreme, enabling real-time Pre-emptive Cyber defence.

- Non-reactive. Defends first; detects later.
- Neutralizes any attack, including unknown zero days, and insider threat actions in seconds to minutes.
- Provides self-defending, automated protection across all IT layers.
- Designed to thwart elite nation-state level attacks, including supply chain, fileless malware, AI and even quantum-enabled threats.
- Execution of security functions separated and isolated by multiple layers from the security control plane/.

Factors Driving the need for Pre-emptive Cyber Defence

- Proliferation of advanced cyber weapons; nation-state developed tools increasingly fall into the hands of well-resourced and interconnected criminal gangs.
- Enterprise-firewalls can now be compromised in seconds-to-minutes, and used as proxies to gain access or attack networks assumed to be hidden and isolated from the outside.
- Insider threats remain an unpredictable and serious risk – even in the most secure environments.
- Cyber effects increasingly used as “Grazy Zone Warfare” to influence, intimidate, and destabilize populations and governments.

- Adversarial AI generates offensive cyber tools faster than even the best defensive technology and can analyse an counter.

Clearly, it is no longer enough to react quickly to a cyber attack, or even prepare in advance via proactive measures. The state of offensive cyber technology today, and in the future, necessitates forward-leaning defence, capable of breaking the attackers kill-chain *before* a cyber effect can successfully establish persistence and begin to execute.

Disruptive Technologies

Cyemptive Technologies deliver the forward-oriented, pre-empted cyber defence needed against today's sophisticated actors. Enterprise solutions incorporates a core of 8 patented technologies, that, in combination, enable:

CyberSlice®

- Automatically isolates attackers, with zero impact on authorized users. Self-healing.
- CyberSlice operating systems, applications, services, files and more in seconds or minutes.
- Operates in the background, transparently, carrying data state across operating systems.

Cyemptive Umbrella Fortress¹

Worldwide, remote network traffic monitoring and response.

- Highly automated passive data flow modelling can back-trace cyber attacks through multiple proxies and onion-routers.
- High-scalable tracers to defeat Bot Nets, defend client data, and expose hackers.

CyberScan / Clean Room Service

Massively (Exabyte-class) scalable forensic file-scanning platform and data transfer platform.

- Seamlessly integrates with and protects existing back-up systems.
- Supports recovery from complex cyberattacks by identifying data abnormalities indicating malware, steganography, sleeper ransomware, and more.
- Ideal solution for DRaaS providers; back-up services; big-data warehouses, forensic discovery firms, etc.

Integrated Enterprise Ready Solutions

End-to-End Enterprise Fortress Suite covers all major IT domains, at megabyte-to-exabyte scale

- **Network:** Risk-based Blueprints scalable from small-business to defence critical infrastructure and nuclear command-and-control.

¹ Utilized during initial client on-boarding. Continued passive monitoring included in support package, but subsequent manual actions will represent billable hours, and may not be available to all markets and all customers. POA.

- **Perimeter:** Dynamic firewalls, with separation of execution and control.
- **Endpoint:** Multi-level secure VPN, encryption, auto-recovery.
- **Cloud:** Secure, sovereign-cloud blueprint and communications.
- **Data & File:** Enterprise Scanner, File Fortress, Ransomware Fortress.
- **Command Center:** Centralized, policy-based control for automated defences. (Machine-vs.-Machine)

Automated Moving Target defence (AMT)

- Real-time isolation, tracking, and forensic repair across OS, apps, hypervisors, and networks.

Customer Benefits

1. Pre-emptive Protection

- Stops threats **before** they execute, unlike SIEM/SOAR models that react post-compromise, based on sensor data and/or logged events.
- Reduces hacker **dwell time** from months to **seconds**, minimizing data loss and reputational damage—even where deeply-embedded backdoors exist.

2. Operational Efficiency + Cost Savings

- Fully automated threat response reduces human overhead.
- Virtually eliminates false positives and manual triage delays.
- Avoids high costs of incident response, SOC escalation, and downtime.
- Massive cost saving via greater integration and few point solutions.
- Competitively priced, protection that outperforms top-selling point solutions on the market

3. Future-Proofing

- Defends against **AI and quantum threats**, which legacy tools struggle to detect.
- OT/IoT, secure communications, including unpatched legacy systems.

4. Zero Trust Architecture

- Assured, auditable Zero Trust and Least Privilege configuration, centrally managed and continuously enforced by CyberSlice®.
- Delivers unmatched data-sovereignty and compliance visibility for clients subject to strict security standards like GDPR, DORA and NIS2.

Competitive Advantage

Cyemptive's **Pre-emptive defence** delivers superior **ROI, Risk Reduction and Resilience** via:

- **Speed:** defeats Known AND unknown threats in seconds to minutes.
- **Automated defence:** machine-vs-machine with human control.
- **Compliance:** policy-enforced compliance with minutes-based reporting.
- **Self-healing:** with enterprise-grade cluster management
- **Data Sovereignty:** multi-data center, off-line, private sovereign cloud.