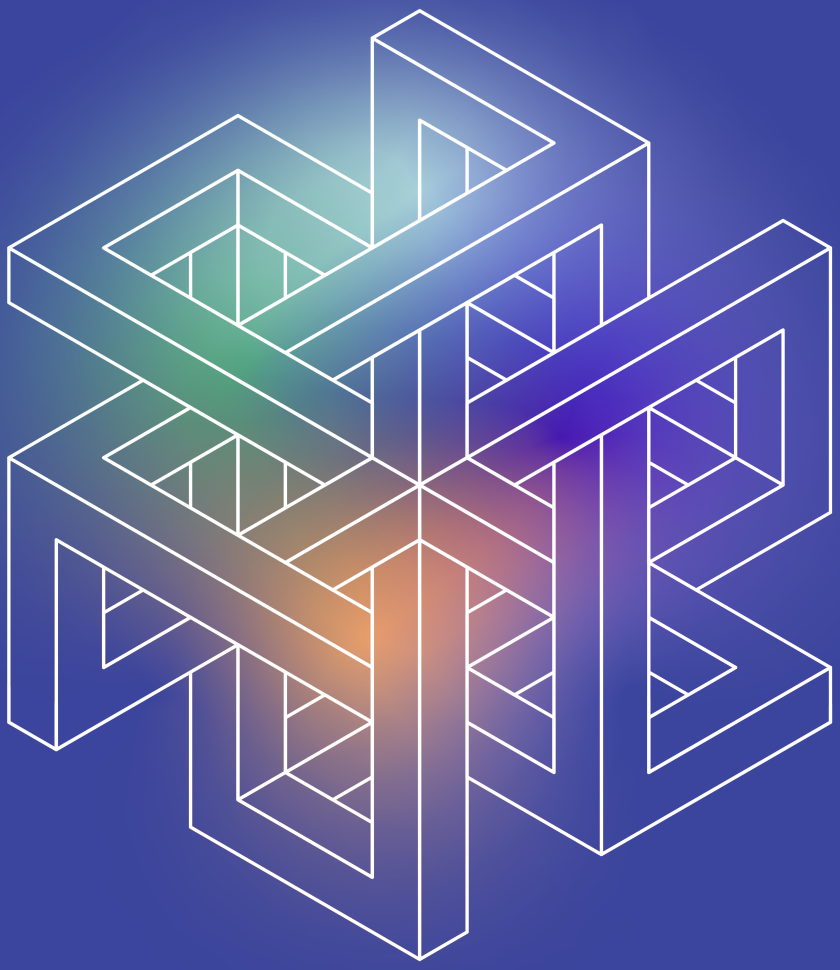


CAPZUL TECHNOLOGY OVERVIEW

CAPZUL

TABLE OF CONTENTS

CAPZUL

EXECUTIVE SUMMARY

- Capzul inverts the usual model: instead of defending exposed systems, it removes the external attack surface entirely.
- Application sessions (e.g. HTTPS) are encapsulated into Capzul's monolithic post-quantum, keyless transport (CNCP), providing peer-to-peer encryption, mutual authentication, and private connectivity without extending the LAN.
- The Capzul Security Engine (CSE) hardens endpoints with anti-reverse engineering, dynamic code obfuscation, and runtime protections, making compromise vastly more difficult
- CapzulLink + Front-end hide servers, use alternative name-to-route resolution (with no public DNS reliance), and admit only CNCP.
- Operationally lightweight yet deeply secure: no public IPs, no open inbound ports, no DNS targets, and no replayable session data. All of it while applications continue speaking standard protocols like HTTPS.

This paper outlines Capzul's security approach, the core pillars that make it possible, and the operational elements used in deployments.

BUSINESS ADVANTAGES WITH CAPZUL

- Near zero downtime: Deployments and upgrades require no code changes, firewall adjustments, or service interruptions.
- Lower risk and impact: With no public-facing assets, the chance and severity of security incidents drop sharply.
- Reduced operational burden: You eliminate much of the complexity associated with TLS, VPNs, PKI, certificate management, and emergency fixes.

Capzul turns network security inside-out, embedding robust protection in the communication layer itself. This gives organizations a resilient, minimal-footprint security foundation.

WHY A DIFFERENT MODEL IS NECESSARY

Attack surface inflation continues: every exposed IP, open port, DNS entry, and TLS endpoint becomes a probe target. In response, organizations stack more controls, but that sprawl drives complexity, operational burden, and new failure modes. At the same time, post-quantum and supply-chain risks demand stronger-by-design assumptions, where endpoints are treated as compromised by default and security is architected to withstand it.

Capzul's thesis is that the safest system is one that cannot be reached directly. Security should not depend on hiding flaws behind layers. It should preclude reachability and verify every step of communication and execution.

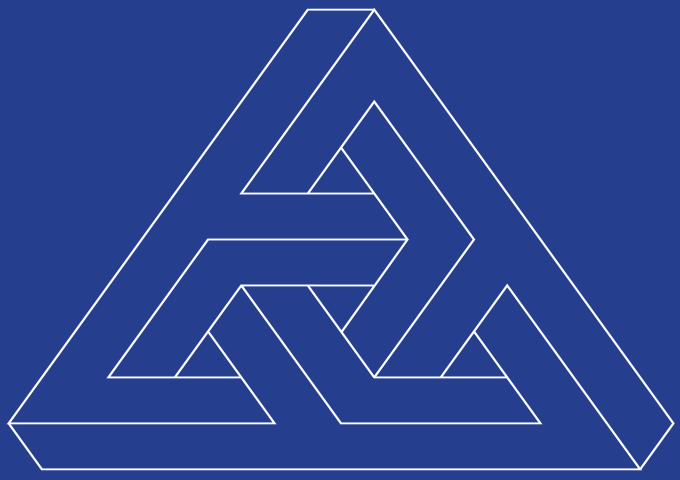
CAPZUL'S SECURITY APPROACH

No public exposure: Servers are not addressable from the Internet; inbound communication is admitted only as CNCP frames via a Capzul Link and delivered to a Front-end on a private interface.

Application-session transport (not VPN tunnels): Capzul encapsulates application sessions (e.g., an HTTPS connection) into CNCP; it does not extend subnets or create
L2/L3 tunnels.

Self-defending runtime: Capzul binaries run under the Capzul Security Engine (CSE), polymorphic code, device-bound cryptography, active traps, and attestation block reverse-engineering and key theft even on compromised hosts.

The Results are Clear:
A hidden infrastructure with authenticated communication, and seamless integration as servers keep speaking standard HTTPS.



CORE PILLAR #1: CAPZUL NETWORK COMMUNICATION PROTOCOL (CNCP)

WHAT IS IT?

CNCP is Capzul's proprietary, monolithic transport: a post-quantum, zero-trust alternative to the TLS/VPN/PKI stack. It provides a single authenticated, encrypted communication mechanism featuring patented ephemeral multi-key handshakes, symmetric bulk encryption, Sequential Keyless Transport (SKT) for validation without decryption, dynamic headers, and rolling MACs. CNCP does not rely on public DNS or exposed ports; only CNCP frames are admitted past a Capzul Link. The Front-end un-capsulates CNCP and forwards unchanged HTTPS to the protected service. All of it while reserving protocol integrity without turning the server into a CNCP speaker.and verify every step of communication and execution.
A key design feature is CNCP's high degrees of freedom: instead of depending on a single large static key, CNCP derives equivalent unpredictability from tight endpoint synchronization and micro-timed sequencing expressed directly in code. That entropy is further amplified by Capzul's high-entropy number generation. This gives our technology symmetric-level protection with asymmetric-style functionality, without the overhead and fragility of certificate hierarchies.

HOW DOES IT WORK?

Ephemeral, multi-key session start. Multiple asymmetric key pairs are generated locally, used briefly, then discarded. Handshake runs inside an authenticated channel with no public certificates or PKI.

Symmetric payload + SKT: After session setup, payloads are encrypted with high-speed symmetric ciphers and carried inside Sequential Keyless Transport. This allows Capzul Links to authenticate, sequence, and route frames without decrypting the application content.

Dynamic headers & rolling MACs.: CNCP mutates header layout per session and stamps frames with rolling MACs tied to session state and ordering. Replays/injections die at the perimeter.

Alternate address resolution.: CNCP uses name-to-route mechanisms independent of public DNS, removing domain hijacking and cache-poison paths.

Only CNCP at the edge; unchanged HTTPS inside. The Link admits CNCP only; the Front-end un-encapsulates and hands the original HTTPS to your server.

This results in a perimeter that exposes nothing. End-to-end confidentiality and authenticity is ensured with no external PKI/VPN stack.

CORE PILLAR #2: CAPZUL SECURITY ENGINE (CSE)

WHAT IS IT?

CSE is Capzul's runtime security engine embedded in all Capzul binaries. It delivers polymorphic code transformation, device-tied encryption, AI-placed behavioral traps, and local/optional remote attestation. Even if a host is fully compromised, Capzul logic and keys cannot be extracted or repurposed.

HOW DOES IT WORK?

RUNTIME CODE MUTATION

On every launch, code shape changes (basic-block reordering, opaque predicates, dummy paths, encrypted control-flow). Static/dynamic analysis yields no durable insight.

ACTIVE TRAPS WITH AI PLACEMENT

Tamper/debug attempts trigger policy-driven countermeasures (terminate, quarantine, corrupt output, alert).

DEVICE-BOUND CRYPTO & GUARDED MEMORY

Binaries are encrypted at rest and decrypted only into guarded runtime pages using hardware-unique anchors (TPM/Secure Enclave/silicon IDs). Copies do not run elsewhere.

ZERO-TRUST ATTESTATION

CSE validates its own code and context before participation; in high-assurance modes, it can prove integrity remotely.

This approach ensures that the endpoint, which is the usual weak link, becomes a self-defending enclave for Capzul operations.

ENABLING ELEMENTS USED IN DEPLOYMENTS

CAPZUL CLIENT

Encapsulates application sessions (e.g. HTTPS) into CNCP. Two typical placements:

- **Local Client (on-prem/LAN):** encapsulates sessions and sends directly to a nearby Capzul Link; no reliance on public IPs/NAT changes.
- **Remote Client (via Capzul Remote):** for external users/systems; HTTPS is encapsulated into CNCP at the edge before traversing the Internet.

All Client binaries are protected by CSE.

CAPZUL LINK

A network node at the perimeter that admits only CNCP frames, authenticates and sequences them (via SKT and rolling MAC), and routes across the Capzul overlay. It uses alternative name-to-route resolution (no public DNS), and does not expose the server's address, ports, or protocol details.

CAPZUL FRONT-END

Software in front of (or on) the protected server that removes CNCP and forwards unchanged HTTPS to the application. This preserves all app-layer behaviors, certificates, and integrations internally with no code changes to your service.

ENCAPSULATION OF APPLICATION SESSIONS:

The Client (or Capzul Remote) wraps the HTTPS session inside CNCP. Links authenticate and route without decrypting HTTPS. The Front-end unwraps CNCP and hands the original HTTPS to the server on a private interface. Only CNCP crosses the public network; the server remains invisible.

SECURITY & BUSINESS OUTCOMES

NO EXTERNAL ATTACK SURFACE

No public IPs and no open inbound ports remove direct probing. No DNS entries to poison eliminates common misdirection paths. There is no direct route to scan or exploit.

ENDPOINT RESILIENCE

CSE prevents reverse engineering and key theft, even on compromised hosts. This limits lateral movement, protects credentials and session material, and reduces incident blast radius, which lowers containment and recovery costs.

POST-QUANTUM, ZERO-TRUST TRANSPORT

CNCP's ephemeral multi-key handshakes, Sequential Keyless Transport, dynamic headers, and rolling MACs protect sessions without the fragility of certificate hierarchies or traditional VPNs. This reduces the probability of session-layer incidents and compresses their duration when they occur, improving mean time to recover and reducing downtime exposure.

OPERATIONAL SIMPLICITY

A single coherent transport and runtime model reduces policy surface area, certificate lifecycles, and emergency changes. Teams spend less time on VPN upkeep, certificate renewals, and perimeter patching, which lowers ongoing operational expense and frees capacity for higher-value work.

SEAMLESS INTEGRATION

Applications continue to use standard HTTPS internally. Deployments require no code changes and minimal network changes. This shortens rollout timelines, avoids planned maintenance windows, and reduces change-related downtime that would otherwise impact revenue and customer experience.

DEVICE-BOUND CRYPTO & GUARDED MEMORY

Binaries are encrypted at rest and decrypted only into guarded runtime pages using hardware-unique anchors (TPM/Secure Enclave/silicon IDs). Copies do not run elsewhere.

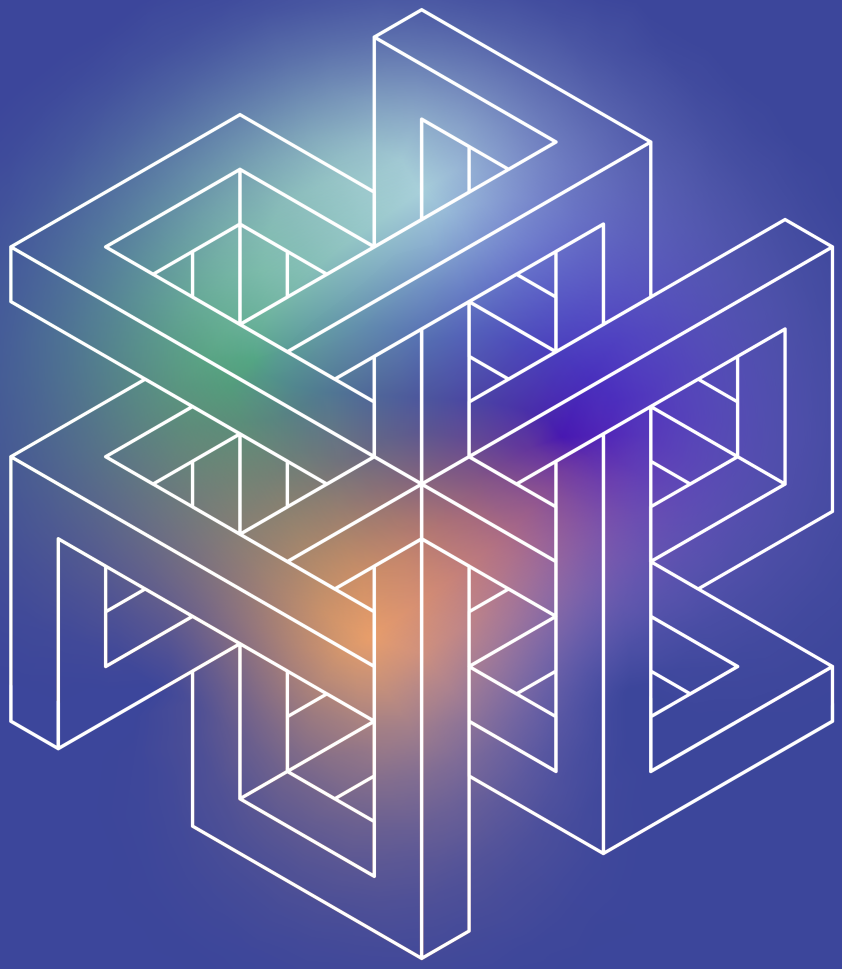
GOVERNANCE, RISK & COMPLIANCE NOTES

Segregation of duties: CNCP transport and CSE runtime controls are enforced by design, independent of perimeter firewalls and IAM systems.

Change management: Migration does not require app rewrites; introduce CNCP/Front-end in front of existing services and phase policies.

Auditability: CNCP admits only authenticated CNCP frames; Links can emit decision logs (admit/drop, sequence validation, route selection) without exposing sensitive payloads.

Resilience posture: Removal of public exposure reduces the likelihood and blast radius of common incidents (port scans, DNS hijacking, credential replay, TLS termination defects).



CAPZUL'S APPROACH TO SECURING AI NETWORKS AND PROPRIETARY DATA

By Incorporating Capzul's Solutions a Large, Multinational Enterprise with an Expanding Network of AI Agents Has Successfully Secured Its Critical Network Infrastructure and Confidential Data from Evolving Threats.

CLIENT PROFILE

The global enterprise's deployment encompassed an ever-expanding network of AI agents, each requiring secure and seamless intercommunication.

These agents were set up to communicate using the open standard Model Context Protocol (MCP). This protocol, leveraging HTTP and a client-server architecture, allows the agents to operate seamlessly across diverse environments, including clouds, data centres, and behind Network Address Translations (NATs).

However, this architecture exposes the AI agents' servers to the public internet, creating a significant external attack surface. This vulnerability makes the system susceptible to threats like port scanning, DDoS attacks and many more.

THE CHALLENGE

Traditional perimeter-based security tools, such as firewalls, together with legacy remote-access solutions like VPN's, were deemed insufficient. They add latency and complexity to the network while still leaving ingress points exposed.

Given these limitations, the core security requirements were:

- **Endpoint Integrity:** Each AI agent must be shielded from unauthorized access and external targeting.
- **Secure Communication:** All data transferred between agents must be fully encrypted and impervious to interception.
- **Scalability & Ease of Deployment:** The solution needed to be easily integrated across a large, distributed network without complex firewall rule changes or network reconfigurations.

EXECUTIVE SUMMARY

INDUSTRY

- Technology / AI agents at scale

ENVIRONMENT

- AI agents communicate via MCP across clouds/DCs/NAT
- Agent <-> agent and agent <-> external data sources; zero-downtime constraint and no app changes requirement.

CHALLENGE

- MCP over HTTP leaves agent services publicly reachable, driving port-scanning/DDoS exposure
- Perimeter tools (VPNs/firewalls) add latency and cert/patch churn and expose ingress
- Need for post-quantum, zero-trust protection for agent traffic and services without network reconfiguration

RESULTS

- Attack surface 0:
- CapzulProtect makes MCP services publicly non-addressable
- Secure data-in-transit creating authenticated links for endpoint<->server / sever<->server over the internet without extending the network
- Operation simplicity: lightweight agent, no firewall changes, no downtime

THE CAPZUL SOLUTION

Capzul provides a paradigm-shifting approach to cybersecurity by eliminating the external attack surface entirely. Capzul deployed its CapzulConnect solution to address these challenges. This innovative, software-based architecture provides a comprehensive security layer that is both highly effective and operationally efficient. The core of the solution lies in the deployment of a Capzul Frontend on each AI agent. CapzulConnect establishes a "stealth tunnel" utilizing its proprietary CNCP (Capzul Network Communication Protocol). This protocol creates a secure, encrypted overlay network that operates over the public internet. This architecture offers several key technical advantages:

- Post-Quantum Point-to-Point Encryption: CapzulConnect encapsulates all data traffic between agents with advanced, post-quantum encryption. This ensures that even with the advent of quantum computing, the encrypted data remains secure.

- Invisible Endpoints: By forgoing conventional DNS and open ports, the solution renders each AI agent virtually invisible to external reconnaissance and attack vectors. This proactive measure prevents intruders from locating or targeting the endpoints directly.

- Zero-Configuration Deployment: The software-based frontend eliminates the need for complex network or firewall reconfigurations. Once installed, AI agents can immediately and securely communicate with other agents on the network, streamlining deployment and maintenance.

CAPZUL TECHNOLOGY

WHAT IT IS

- Zero-trust, post-quantum connectivity that keeps services publicly non-addressable preserving application protocols

SOLUTIONS

- CapzulProtect: server cloaking: no routable IPs, no inbound ports, no public DNS; access only via authenticated CNCP.
- CapzulConnect: ultra-secure endpoint<->app / server<->server data transport over the internet without extending the network.

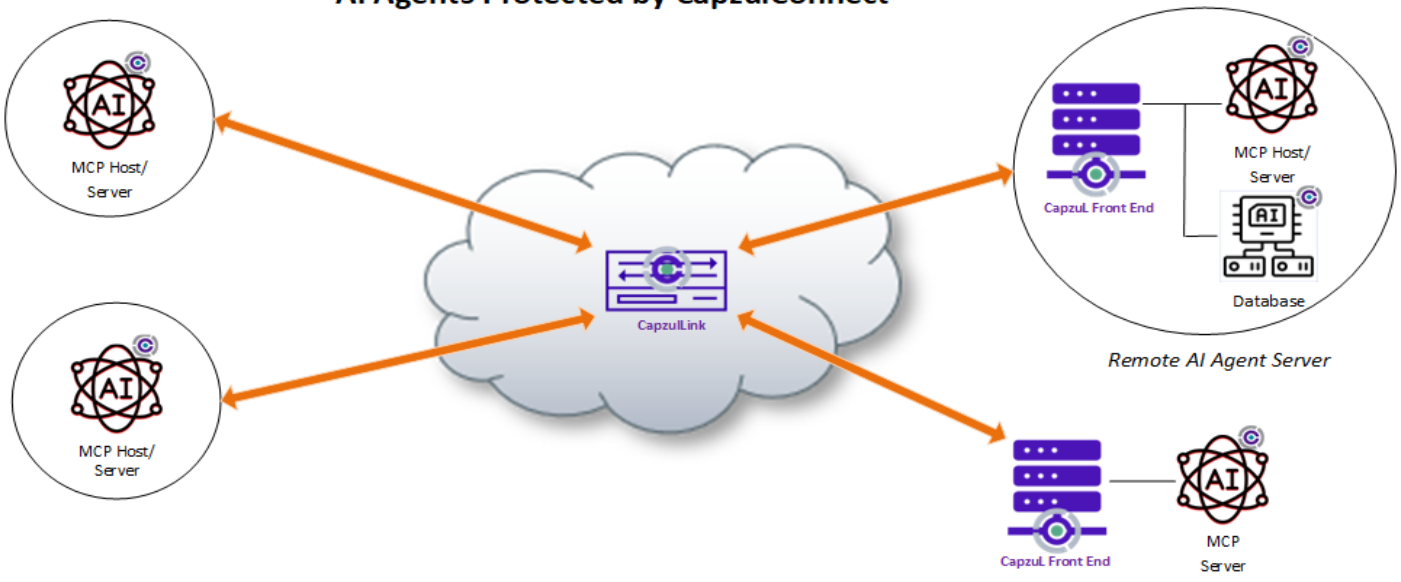
DEPLOYMENT

- Seamless integration. Lightweight agent, no firewall changes; works across clouds/DCs/NAT with OTA policy and crypto rotation.

OUTCOMES

- External attack surface <-> 0; least privilege point-to-point access.
- Fewer appliances/tickets (no VPN/PKI sprawl), lower TCO, simpler audits.
- Greater agility: move services/data without reopening the network.

AI Agents Protected by CapzulConnect



KEY BENEFITS AND BUSINESS VALUE

- Elimination of the External Attack Surface: By implementing the CapzulConnect solution, the client completely removed the external attack surface for each of the AI agents providing a level of security that goes beyond traditional firewalls or VPNs.

- Quantum-Safe and Future-Proof Security: Capzul's solutions use post-quantum-ready cryptography to encapsulate and hide all traffic. This ensures the client's AI communication is protected not just from today's threats, but also from the future risk of quantum-based attacks.

- Seamless Integration and Simplified Management: CapzulConnect was easily implemented for an expanding network of AI agents which did not require code changes or complex reconfigurations. This enabled the organization to safeguard critical systems with minimal operational overhead, freeing up resources spent on managing traditional security tools and chasing threats.

CONCLUSION

By implementing the CapzulConnect solution, the client achieved a level of security previously considered unattainable. The organization's security posture transitioned from reactive, perimeter-based defences to a proactive, attack-proof environment. The AI communication, data, and servers are now fundamentally protected by a security model that eliminates vulnerabilities at their source.This solution simplifies network management by enabling the rapid, frictionless introduction of new AI agents without the time-consuming and complex methods typically required for network infrastructure changes. This operational agility allows the client to preserve brand reputation, focus on innovation, and confidently trust that their AI ecosystem is secured against both present and future cyber risks.

CAPZUL TECHNOLOGY

ENERGY & UTILITIES

- Substation/RTU gateways; historian links

MANUFACTURING & INDUSTRIAL

- MES/PLC gateways; vendor maintenance access

MINING & NATURAL RESOURCES

- Pit/plant edge; LTE/VSAT telemetry backhaul

TRANSPORTATION & LOGISTICS

- WMS/TMS to cloud; scanners/telematics

HEALTHCARE & LIFE SCIENCES

- EMR/LIMS security; PHI/telehealth APIs

GOVERNMENT & DEFENSE

- Enclave<->enclave exchange; C2/sensor nets

TELECOM / 5G / MEC

- MEC app protection; UE<->edge<->core paths

FINANCIAL SERVICES

- Core banking APIs; branch<->core connectivity

SMART CITIES / IOT

- Sensor/CCTV backhaul; utility telemetry

SAAS / CLOUD PROVIDERS

- Customer microservices; region<->region data planes

EDUCATION & RESEARCH

- Lab<->HPC/cloud; shared research data