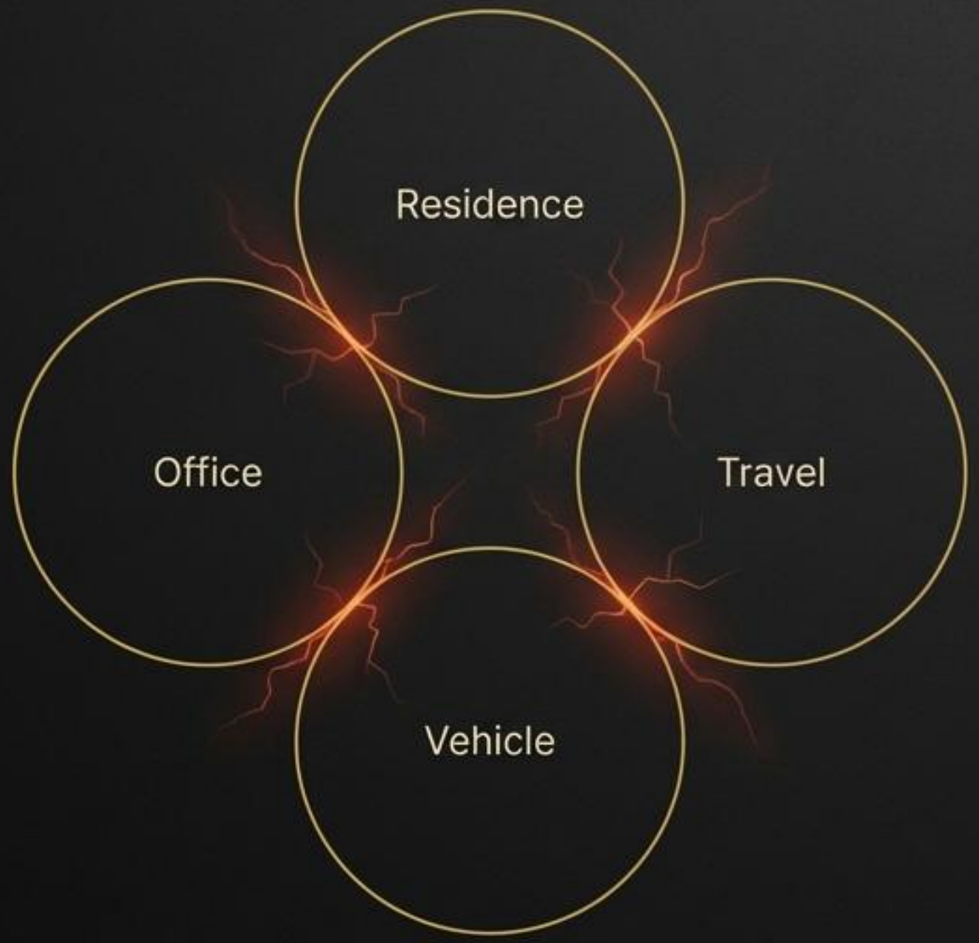
GREENJAY

Engineering a Protected Life.

The Failure of Conventional Security is Not in its Components, but in its Seams.



Most security failures in ultra-high-net-worth environments do not happen because a client lacked cameras or guards. They happen because systems were acquired as isolated purchases, installed by separate vendors, and never engineered into a single operating standard.

One vendor optimized for convenience. Another for aesthetics. A third for response. Nobody owned the seams between them.

In UHNW environments, the seams are where compromise becomes possible.

The Secure State

An engineered condition where lifestyle systems remain elegant and usable, privacy remains intact, and security remains verifiable.

It is not a product or a bundle. It is an operating standard established through governance, technical assurance, and unified oversight.

One Standard, Applied Across Every Domain of Life.

Your protection environment is not one environment. It is multiple environments stitched together by routine. Our methodology applies a single, defensible operating standard that spans both physical and digital systems across three critical domains.

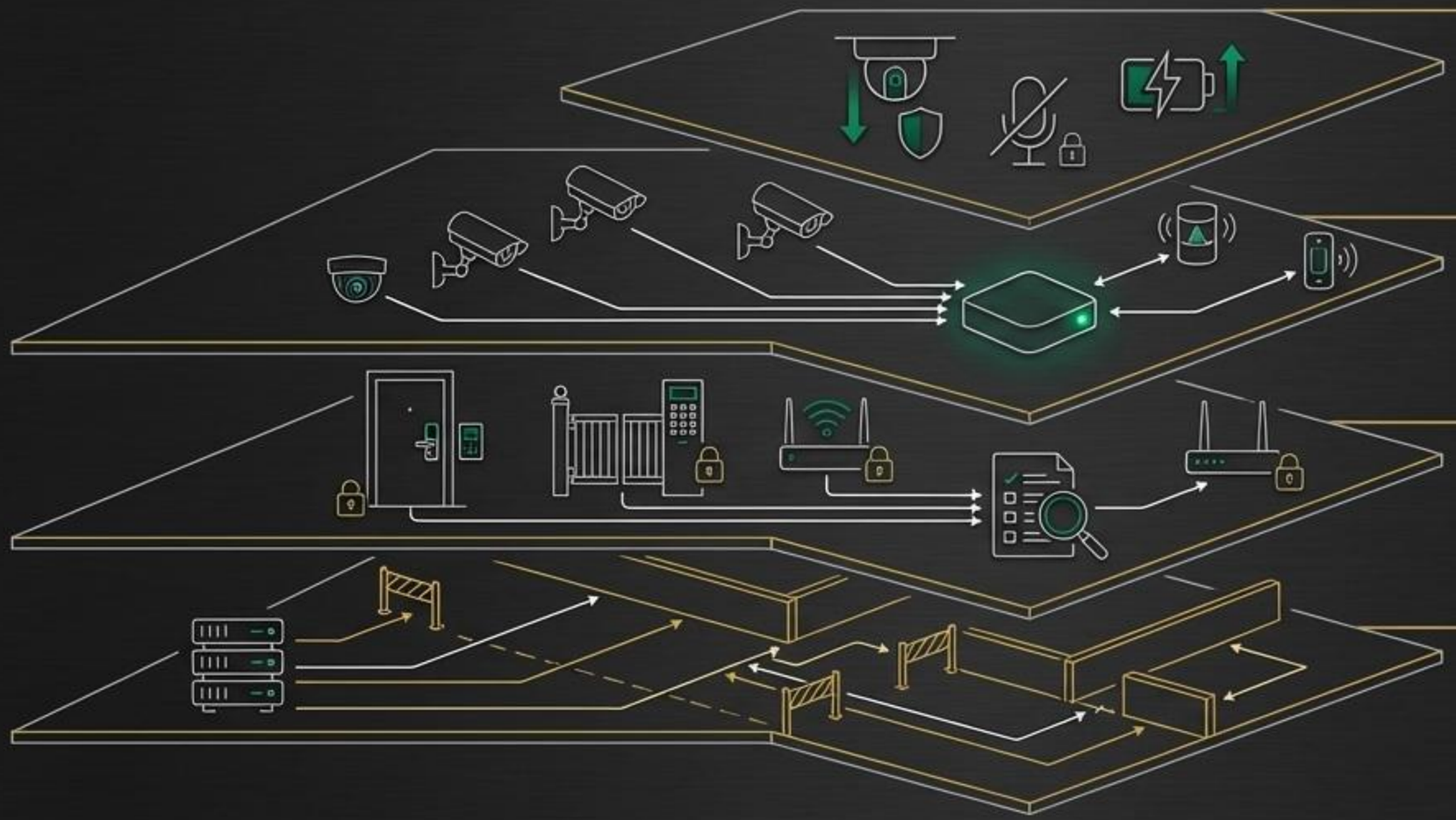
The Estate: Hardening the technological and physical heart of your life.

Transitions & Travel:
Protecting the spaces between secured environments.

Communications & Connectivity:
Ensuring the integrity of your information layer.

The Secure Estate: Engineering Integrity with Aesthetic Restraint

Luxury estates are technology estates. Lighting, AV, access, and surveillance are interconnected. Convenience can become exposure if not governed. Our approach hardens the estate through four distinct, integrated layers.



Resilience & Privacy

Engineered to operate through outages, with built-in privacy controls like retractable cameras and muted microphones.

Monitoring Integrity

Integrated, verified, and actionable monitoring that eliminates false alarm fatigue and silent failures.

Access Governance

A living access model with controlled windows, accountability logs, and revocation discipline for all staff and vendors.

Architecture

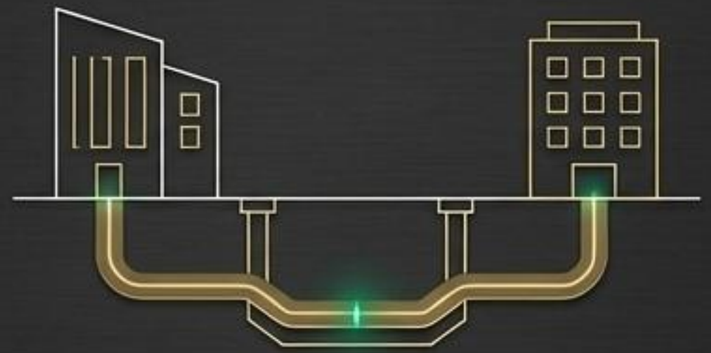
Network segmentation that prevents compromise. A guest device must never provide a pathway to security cameras.

Secure Logistics: Protecting Transitions Without Disrupting Life.

Risk exists in the spaces between secured environments. True logistics is more than cars and drivers; it is the choreography of movement that reduces observable patterns and minimizes exposure windows.

Mobility Governance

A disciplined system that treats movement as an operational process, integrating vehicles, drivers, communications, and contingency planning.



Basement-to-Basement Protocols

Ensuring a secure, controlled transition from one trusted environment to another.

Discreet Reliability

A high-end logistics posture should not feel like a security operation. It should feel like a private service with exceptional, engineered reliability.

Advance Operations: Engineering the Condition of Arrival

Arriving early is not enough. True advance operations is an engineered reduction of uncertainty. It is about preventing invisible decisions from controlling your risk before you even arrive.

1. Environment Validation

Verifiable physical and digital checks to confirm an environment is what it claims to be—from suite privacy to network integrity.

2. Personnel Alignment

Governing the access model for all staff, vendors, and contractors to ensure accountability.

3. Communications Assurance

Establishing continuity of secure communication, independent of untrusted hotel Wi-Fi or variable carrier coverage.

4. Continuity Oversight

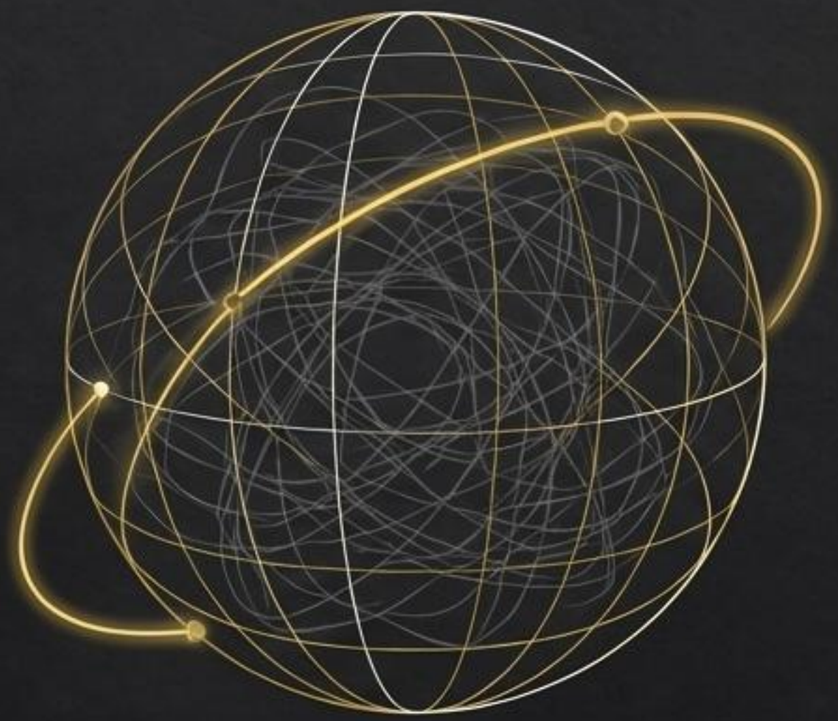
Quietly managing changes post-validation to ensure the environment remains secure without friction or disruption to the principal.

Command & Control: The Unifying Layer for a Quieter Life.

Command & Control is the layer that turns components into a coherent operating system. Its value is not in adding more monitoring, but in adding governance. It provides a single, accountable location where events are interpreted, verified, and handled.

Calm Escalation. Chaos is reputational damage. Overreaction is disruption. Underreaction is exposure. Our oversight layer operates privately, escalating only when verified conditions justify action.

Secure Connectivity: A Private Network, Anywhere You Go



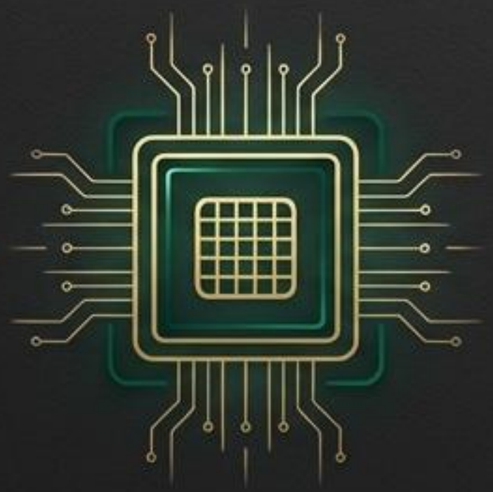
The most common communications risk is not cracked encryption; it is being forced onto untrusted networks. Our private network capability creates a trusted path for your data, turning any carrier or Wi-Fi network into your own secure edge.

- Zero Trust Architecture: Securing untrusted environments like hotels and airports.
- Private Global Routing: Your mobile traffic is routed privately, regardless of the local carrier.
- Centralized Governance: Real-time control, management, and auditing of all connected assets.
- Infrastructure Integrity: Ensures the protective team and command center maintain stable, secure connectivity for coordination and oversight.

Intelligent Systems: Signal Clarity, Not More Alerts

Artificial intelligence is a powerful tool for strengthening the Secure State. Our application of AI is focused on signal clarity, anomaly recognition, and faster verification with less disruption.

RAW DATA



AI ANALYSIS

Detection Quality: Moving beyond raw footage to identify relevant events—person detection, perimeter anomalies, intrusion patterns—that produce better intelligence, not more alarms.

Governed Recognition: Using classification (friendly/unknown) under strict cllent consent and privacy protocols to reduce uncertainty about activity on the estate.

Calm Escalation Assistance: Correlating signals from multiple sensors (access, cameras, networl() to verify threats before escalating, preventing overreaction and preserving quiet.

Sustained Assurance: A Governance Wrapper for a Lifetime.

A Secure State is not static. It must be maintained. Access accumulates, vendors change, staff turns over, and technology evolves. Our engagement model provides a governance wrapper to ensure the standard remains true over time.

Documentation an office can retain and audit.

Governance Rules that define access and oversight.

A Sustainment Plan for continuous integrity.

Security is not the acquisition of equipment and personnel.

It is the engineering of a protected life. A state where the household remains elegant, private, and uninterrupted, while security is verifiable, governed, and resilient.

GREENJAY