
GREENJAY
PROTECTIVE GROUP
Where Physical Security Meets Digital Sovereignty.
A Division of GreenJay Technologies LLC | Service-Disabled Veteran-Owned Small Business

Traditional Security Is a Medieval Castle in a Digital Age.

The traditional security model is a fortress with thick walls, high towers, and a strong gate. It focuses all resources on hardening the destination. But it ignores two critical, modern realities:

1. The **unprotected roads** leading to the castle, where vulnerability is highest.
2. The **dust clouds** your caravan kicks up, announcing your patterns, intentions, and vulnerabilities to any adversary watching from a distance.

Your Lifestyle Is a Broadcast Adversaries Are Listening To.

The very things that define your life—your public profile, your patterns of movement, your reliance on technology—are broadcasting an "operational signature." This signature allows adversaries to model your life, predict your behavior, and identify points of maximum vulnerability. Social media posts reveal travel schedules. Predictable routes create ambush opportunities. Smart home devices broadcast your presence or absence. Together, they create a complete operational picture. If your life can be modeled, it can be exploited.

68%

OF UHNW FAMILIES REPORT SECURITY CONCERNS

12×

HIGHER TARGETING RATE FOR $50M+ ESTATES

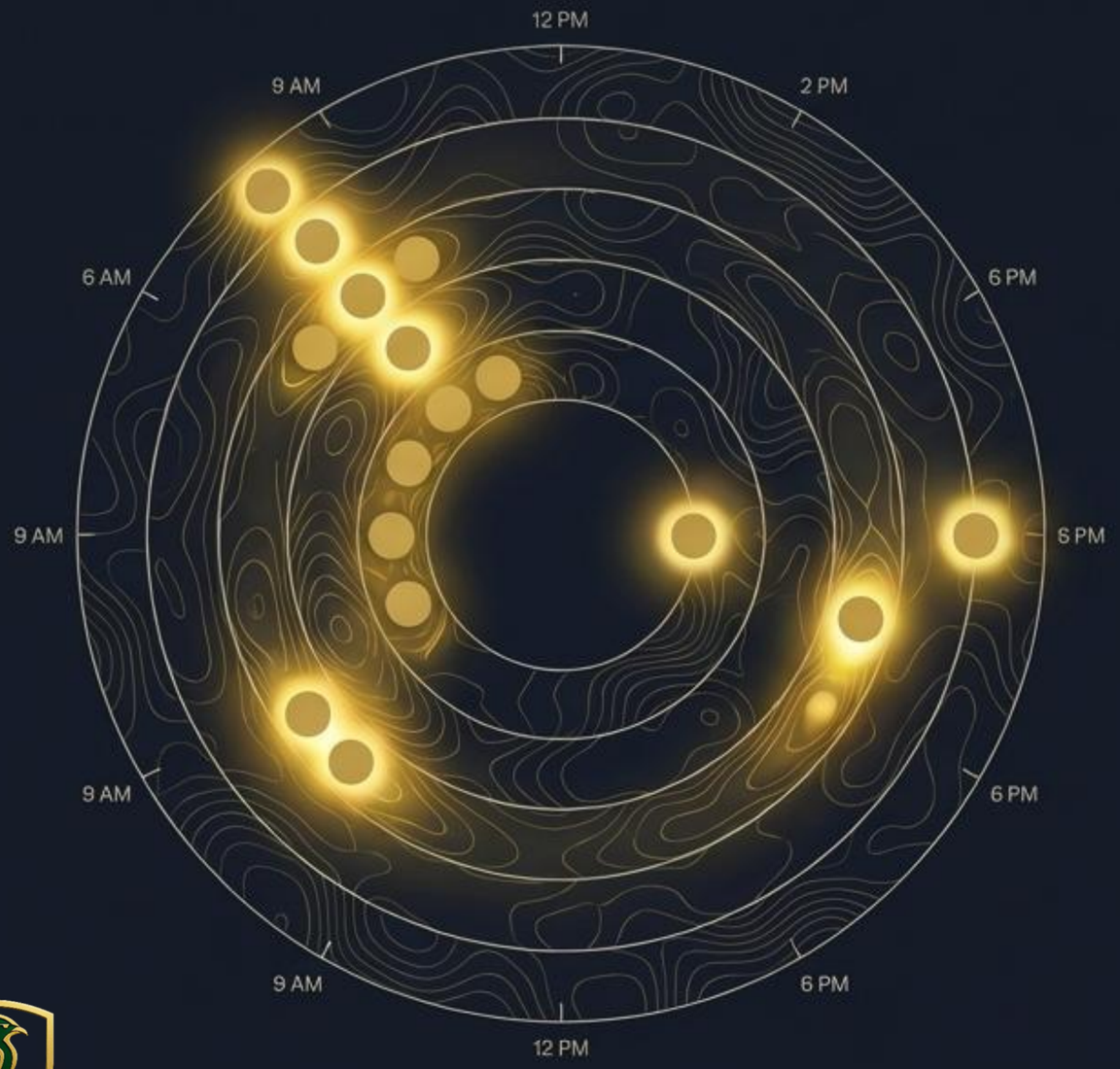
Security Failures Happen in the Seams.

Most security failures don't happen because of a lack of tools. They happen because threats cross boundaries faster than decisions do. Adversaries don't respect departmental silos.

They exploit the seams between your physical security, your cyber defenses, your staff, and your family's routines.

Traditional security approaches treat each domain separately, creating the very fragmentation that modern adversaries are sophisticated enough to exploit with precision.

Their First Target is Predictability.



Before any action, an adversary maps your life. They don't need to hack you; they just need to listen to the "trail" you emit. This is your signature.

- **Pattern-of-Life (POL) Analysis:** Mapping your routines—work, fitness, school runs, social engagements—to forecast your future location.
- **Electromagnetic (EM) Signature:** Tracking the passive "breadcrumbs" from your mobile devices, vehicles, and wearables.

If an adversary watched your life for 7 days, could they predict where you will be in 48 hours? If the answer is yes, the system has failed before it begins.

Their Second Target is the Transition—The “Liminal Spaces.”

The highest statistical probability of a compromise occurs not in your hardened home or office, but in the transitions between them. Adversaries call these liminal spaces.

- **Choke Points:** Locations on your regular routes where your vehicle is forced to slow or stop, creating an ambush or surveillance window.
- **The 30-Second Window:** The moment of maximum exposure when moving from a hardened vehicle to a hardened facility.
- **The ‘Uberization’ of Life:** The constant flow of unvetted third-party services (deliveries, ride-shares) that penetrate your perimeter.

Their Final Target is Trust—The "Inside-the-Wire" Threat.

For an adversary, your most trusted staff—the nanny, the personal assistant, the private chef—are not obstacles. They are human intelligence targets. These individuals have "Total Access" but rarely "Total Loyalty." An adversary's goal is to develop them as a source using the "MICE" framework:

Money: Financial pressure or greed.

Ideology: Political or personal beliefs.

Compromise: Blackmail or leverage.

Ego: Flattery and a sense of importance.

How the Pillars Counter the Adversary's Playbook

Counters Predictability

Pillar: Threat Intelligence

Counters **Predictability** through active Signature Management, Pattern-of-Life variance, and mapping of your digital footprint.

Secures Transitions

Pillar: Physical Security

Secures **Transitions** with dedicated Liminal Space protocols, Trigger Point Analysis, and Transition Drills.

Mitigates Insider Threats

Pillar: Human Security

Mitigates **Insider Threats** with Social Engineering Resistance training, staff Red Teaming, and Compartmentalized Life Management.

Our Doctrine: Integrated Protection

A unified security ecosystem designed to close the seams exploited by modern adversaries.

Threat Intelligence
Understanding the specific threats you face based on your profile, industry, and exposure.

Incident Response
Capability to detect, respond, and recover across physical and digital domains.

Governance Framework
Policy structure enabling sustainable security operations across all domains.

Physical Security
Layered defense that anticipates and adapts to evolving threat patterns.

Strategic Cybersecurity
Protecting digital assets with an 'assume-breach' posture and zero-trust architecture.

Human Security
Transforming people from weakest link to strongest shield through training and culture.

The GreenJay Difference: An Uncompromised Framework

Vendor Neutrality

We do not sell hardware or resell software. Our advice is completely unbiased, driven only by your mission requirements. This ensures every recommendation serves your interests, not our revenue targets.

Compartmentalized Execution

No single vendor or installer ever sees your complete security architecture. The camera installer doesn't know the network design; the network team doesn't see the panic protocols. We maintain OPSEC by design, protecting you from insider threats.

Adversarial Perspective

Our Special Forces background means we think like attackers first. We provide the 'external gravity' to see the whole system and challenge assumptions, identifying vulnerabilities before adversaries do.

Validation Through Adversarial Emulation.

A system is only valid if it survives a simulated attack that hits physical, cyber, and human seams simultaneously. Our operators conduct non-destructive, multi-vector penetration tests of a client's life to provide "Ground Truth" reporting.

"A Real-World 'Seam' Test: 'Can an operator gain digital access to the home's IoT network (Cyber) to disable a physical lock (Physical) by posing as a service technician who socially engineers the staff (Human)?' This is the hard truth we provide."

A Unified Ecosystem of Capabilities

Protection Division

Executive Protection
Low-signature protection by Green Beret-trained specialists.

Advance Operations
24-72 hour advance party deployment for complete environmental control.

Secure Logistics
'Basement-to-Basement' controlled movement to eliminate exposure during transit.

Family Office Advisory
Ongoing security advisor managing complex, multi-generational requirements.

Technology Division

The Secure Estate
Design, Installation, and Hardening of Surveillance Systems, AV, IT, and Smart Home Systems against digital intrusion.

Command & Control
AI-enabled surveillance and unified sensor data for advanced situational awareness.

Secure Communications
Custom protocols and hardened devices to protect conversations from nation-state level adversaries.

Counter-Surveillance (TSCM)
Advanced sweeps to find hidden electronics, even when powered off.

The GreenJay Difference: An Uncompromised Framework

Vendor Neutrality

We do not sell hardware or resell software. Our advice is completely unbiased, driven only by your mission requirements.

Compartmentalized Execution

No single vendor or installer ever sees your complete security architecture. We maintain OPSEC by design, protecting you from insider threats.

Adversarial Perspective

Our Special Forces background means we think like attackers first. We provide the 'external gravity' to challenge assumptions.

Validation Through Adversarial Emulation

A system is only valid if it survives a simulated attack that hits physical, cyber, and human seams simultaneously.

***"A Real-World 'Seam' Test:** "Can an operator gain digital access to the home's IoT network (Cyber) to disable a physical lock (Physical) by posing as a service technician who socially engineers the staff (Human)?" This is the hard truth we provide."*

Advanced Capabilities in Focus: Command & Control

We integrate all camera feeds and sensor data into a unified command interface, enabling proactive protection from anywhere.

- AI-Powered Analytics with Real-Time Threat Detection
- Thermal & Long-Range Telescoping Surveillance (1,000+ meters)
- Drone & RF Detection with Radar Integration
- Facial Recognition & License Plate Capture at 500+ feet
- Unified Command Interface for Fixed and Mobile Operation

Unrivaled Credentials. Proven Excellence.

Federal Agency Relationships

Active contracting relationships with the FBI, Secret Service, and DHS. We apply the same methodologies used to protect classified facilities and high-value government targets.

Security Clearances

Leadership maintains active Top Secret / SCI clearances. Every team member undergoes comprehensive background verification exceeding industry standards.

Elite Certifications

- Service-Disabled Veteran-Owned Small Business (SDVOSB)
- Certified TSCM professionals
- Dignitary protection certifications

Advanced Technical Education

- M.S. in Computer Engineering (Summa Cum Laude) specializing in secure communications and AI.
- B.S. in Criminal Justice providing a foundation in investigative methodology.

The Path to Sovereignty: A Phased Engagement Model

01

Executive Intelligence Baseline

A comprehensive assessment to understand your true exposure, including digital footprint analysis and threat environment mapping. This phase creates the intelligence foundation for all protection decisions.

02

Integrated Protection Design

We architect your complete, vendor-neutral protection system. The output is compartmentalized, ready-to-bid documentation that maintains operational security.

03

Implementation & Training

We oversee installation by vetted subcontractors, maintaining OPSEC throughout. We then provide targeted training for family and staff to transform technology into true protection.

04

Continuous Stewardship

Protection is not a one-time project. We provide ongoing threat monitoring, quarterly intelligence briefs, and regular simulations to ensure your protection evolves as threats change.

“We don’t install security. We steward protection—before, during, and after uncertainty.”

GreenJay operates as vendor-neutral protection stewards, not hardware installers. Traditional security companies profit from selling you equipment, creating inherent bias. Our business model eliminates this conflict. We succeed only when your protection works. This alignment of incentives ensures every recommendation serves your security, not our revenue.

Request a Confidential Briefing

The first step is not to install equipment, but to gain intelligence. We begin with a confidential briefing to understand your requirements and assess your current exposure.

This is not a sales call; it is a strategic discussion of your protection needs.

All inquiries are handled with absolute confidentiality and are protected by a non-disclosure agreement upon request.


GREENJAY
PROTECTIVE GROUP