NIGHTINGALE SECURITY

WHITE PAPER · MAY 2026

Securing Critical Infrastructure for the Autonomous Era

How regulation-aligned, edge-native autonomous security is redefining physical protection for the world's most essential facilities.

Published by
Nightingale Security

Author
Jack Wu, Founder & CEO

Contact
jack@nightingalesecurity.com

EXECUTIVE SUMMARY

Critical infrastructure — the power grids, data centers, airports, ports, and manufacturing facilities that underpin modern civilization — faces a security crisis that legacy approaches can no longer adequately address. Threats are growing in frequency and sophistication. Facilities are expanding in scale. And the regulatory environment is evolving rapidly to demand more capable, cyber-secure, and resilient protection systems.

This white paper examines the converging forces driving the transformation of physical security, analyzes the regulatory frameworks shaping enterprise requirements, and explains how Nightingale's autonomous, edge-native platform is purpose-built to meet these challenges — today, not in some hypothetical future.

SECTION 01

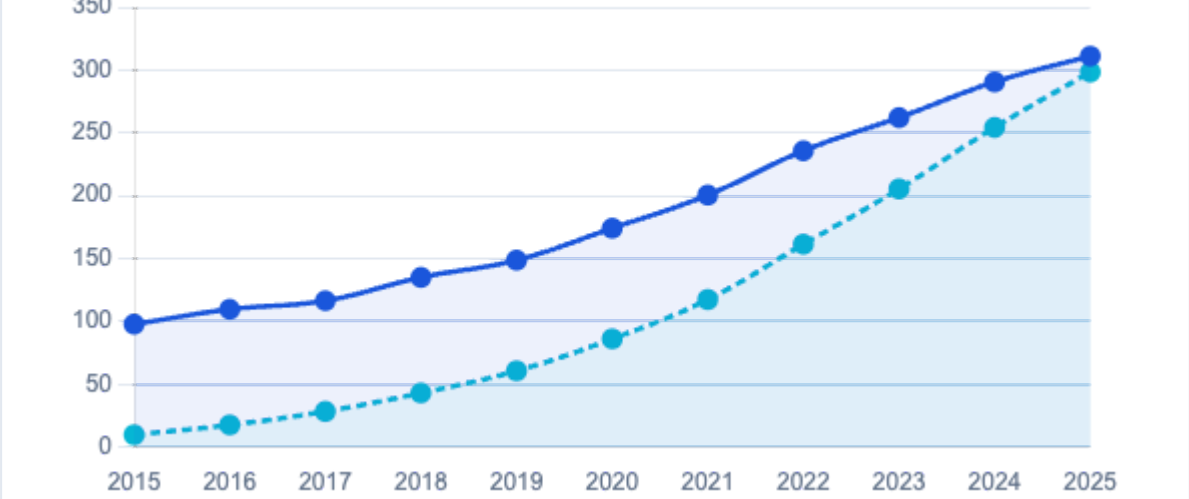
The Escalating Threat Landscape

Physical attacks against critical infrastructure have increased sharply over the past decade. Nation-state actors, organized criminal groups, and domestic extremists increasingly target energy grids, communications infrastructure, transportation networks, and data centers — recognizing that physical disruption can produce cascading effects far beyond the immediate target.

At the same time, facilities themselves are growing larger and more distributed. A modern utility substation may span hundreds of acres. An AI data center campus may consist of dozens of buildings across multiple sites. The perimeter that security teams must monitor and protect is expanding faster than headcount can scale.

Reported Physical Attacks on Critical Infrastructure (Indexed, 2015–2025)

Source: U.S. Department of Energy, DHS Critical Infrastructure Reports (illustrative trend)



Meanwhile, the attack surface is diversifying. Drones, autonomous vehicles, and other emerging technologies are being weaponized or exploited for reconnaissance — creating threats that traditional perimeter cameras and guards are not equipped to detect or counter in real time.

3×
Increase in grid physical security incidents since 2015

74%
Of security leaders say perimeter gaps are their top concern

$1.1T
Global critical infrastructure security market by 2030

<90s
Average time to breach an unmonitored perimeter

SECTION 02

Why Traditional Security Cannot Scale

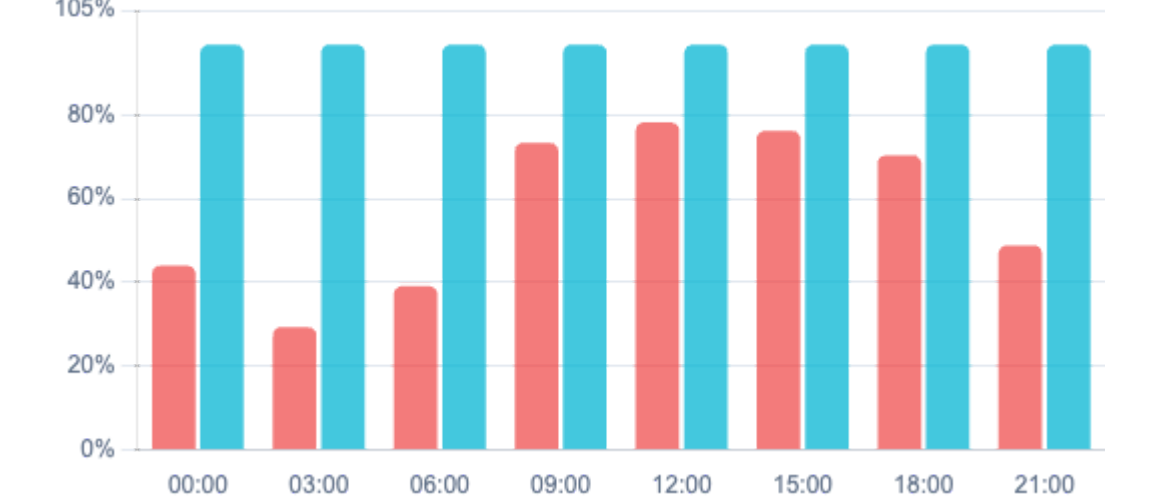
For decades, physical security has relied on a combination of human guards, fixed cameras, and access control systems. These tools were designed for a different threat environment — one with smaller perimeters, lower threat velocity, and less sophisticated adversaries. They were not designed for the scale, complexity, or persistence that critical infrastructure demands today.

> *"Guards can only be in one place at a time. Cameras only capture what they're pointed at. Neither can respond autonomously in real time to a rapidly evolving threat."*
>
> — Jack Wu, Founder & CEO, Nightingale Security

CAPABILITY	TRADITIONAL SECURITY	NIGHTINGALE AUTONOMOUS
Coverage continuity	Shift-based, subject to fatigue and gaps	24/7/365 autonomous operation
Perimeter scale	Linear cost growth with headcount	Scales across large / distributed sites
Threat detection speed	Dependent on human observation & reaction	Real-time autonomous detection & response
Night / adverse conditions	Severely degraded visibility	Thermal imaging, all-weather operation
Cybersecurity posture	Cloud-dependent, vulnerable to network attacks	Edge-native, air-gap capable
Regulatory compliance	Requires costly manual documentation	Automated audit trails and reporting
Alarm verification	Slow, often delayed by dispatch lag	Immediate autonomous visual verification
Operational resilience	Single points of failure (personnel, connectivity)	Resilient edge architecture, degrades gracefully

Security Coverage: Guard-Based vs. Autonomous System (Illustrative 24hr Cycle)

Effective monitoring coverage (%) across a typical large facility



SECTION 03

The Regulatory Imperative

The regulatory environment governing critical infrastructure security is evolving rapidly. Agencies and standards bodies are converging on a common set of requirements: systems must be secure by design, operationally resilient, cyber-hardened, and capable of persistent situational awareness. These requirements don't describe a future aspiration — they describe what regulators expect today.

Nightingale was designed with these frameworks in mind from the start, not retrofitted for compliance after the fact.

CISA GUIDANCE

Cybersecurity & Infrastructure Security Agency

CISA's guidance increasingly recognizes autonomous systems — including drones — as both a potential threat vector and an essential defensive tool. Their emphasis on secure-by-design architecture directly shapes how Nightingale is built.

- → Secure-by-design systems
- → Data sovereignty & edge processing
- → Secure communications architecture
- → Persistent situational awareness
- → Integrated autonomous response capability
- → Cyber-resilient operations

NERC CIP-014

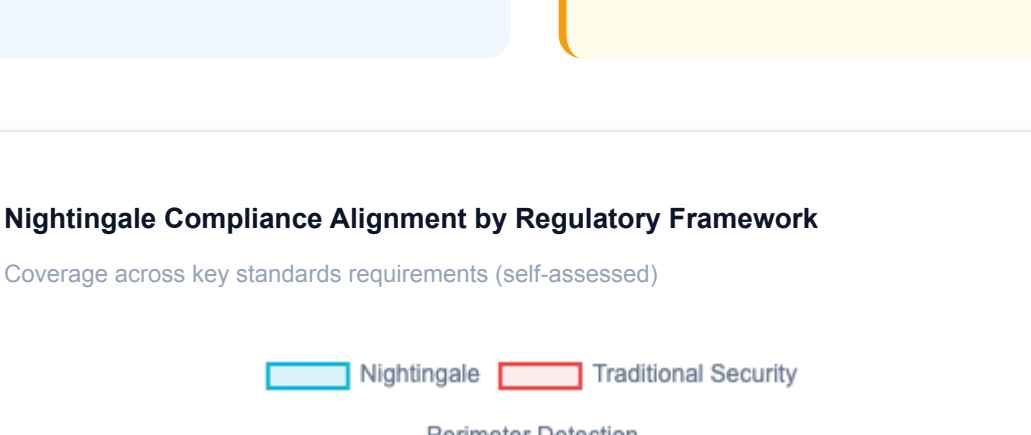
North American Electric Reliability Corporation

NERC CIP-014 mandates that utilities and grid operators implement verifiable, documented physical security programs for high-voltage transmission substations and control centers.

- → Perimeter protection documentation
- → Threat identification & assessment
- → Response plan implementation
- → Third-party plan evaluation
- → Corrective action programs
- → Ongoing audit & review requirements

Nightingale Compliance Alignment by Regulatory Framework

Coverage across key standards requirements (self-assessed)



These requirements are no longer limited to utilities. The same mandate for persistent monitoring, cyber-secure architecture, and documented incident response is spreading to AI data centers, Fortune 500 campuses, advanced manufacturing, and defense-adjacent facilities. Nightingale's architecture anticipates this convergence.

SECTION 04

The Nightingale Platform: Built for the Edge

Nightingale's fundamental architectural principle — that physical AI must operate where the infrastructure exists, not where internet connectivity is assumed — shapes every design decision we make. Our platform runs entirely at the edge, processing data where it is generated, enabling real-time autonomous response without any dependency on cloud infrastructure or reliable network connectivity.

This is not a minor distinction. For operators of critical infrastructure, cloud dependency introduces latency, creates single points of failure, and expands the attack surface available to adversaries. Edge-native architecture eliminates these vulnerabilities by design.

Edge Autonomy
All processing, decision-making, and response happens locally. No cloud dependency. No latency. Full operation in air-gapped or degraded network environments.

Persistent Awareness
Continuous autonomous patrol with thermal imaging enables round-the-clock visibility across large perimeters — day, night, and in adverse conditions.

Autonomous Response
Immediate alarm verification and real-time response without waiting for human dispatch. Threats are assessed and addressed in seconds, not minutes.

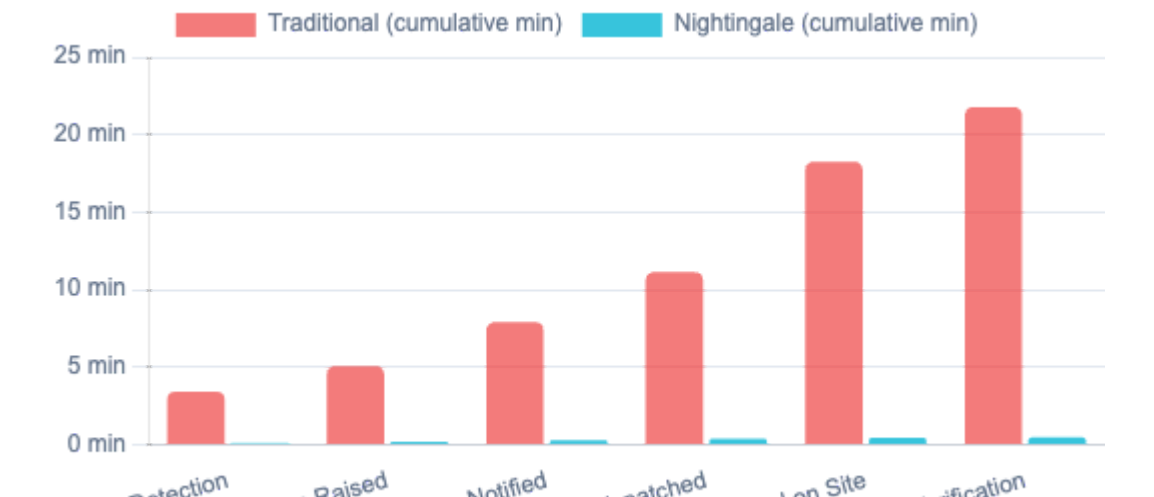
Cyber-Secure Architecture
Designed to CISA's secure-by-design principles. Encrypted communications, data sovereignty at the edge, and a minimal attack surface.

Enterprise Integration
Nightingale integrates into existing security operations — PSIM, SOC workflows, and access control systems — rather than replacing them.

Compliance Automation
Automated audit logs, incident documentation, and reporting tools make regulatory compliance a byproduct of operations, not a separate workload.

Response Time: Traditional vs. Nightingale Autonomous (Simulated Intrusion Event)

Time in minutes from detection trigger to verified response



SECTION 05

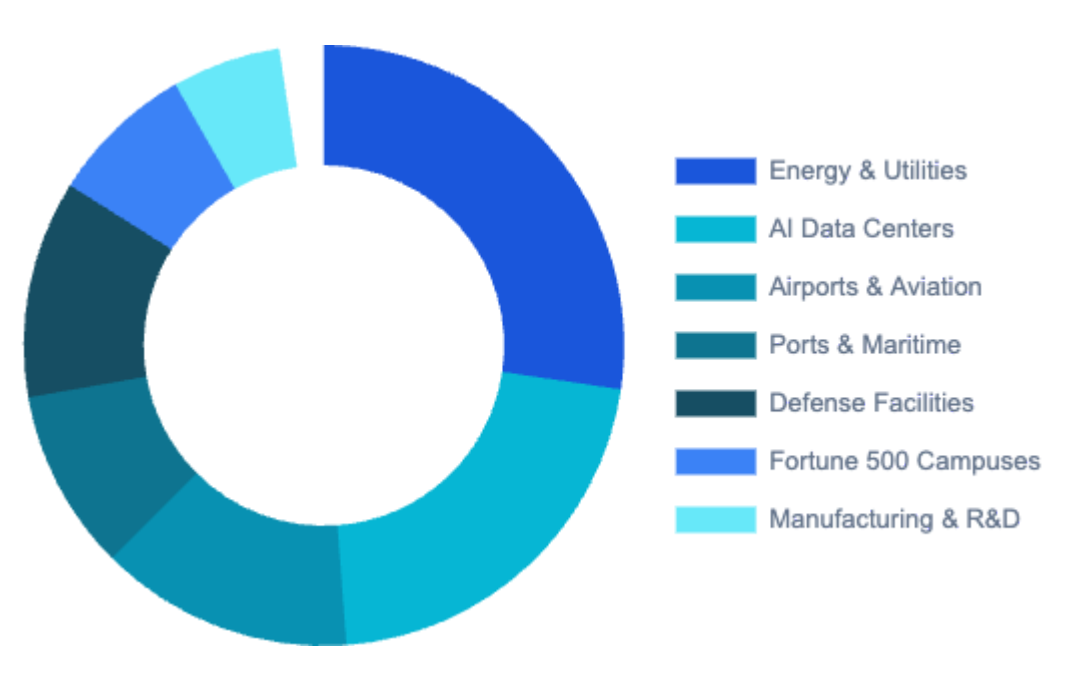
Where Nightingale Operates

Nightingale is purpose-built for environments where operational continuity, physical security, and regulatory compliance are deeply interconnected. Our deployments span the full breadth of critical infrastructure — from energy generation to AI compute, from defense to advanced manufacturing.

Energy & Utilities · AI Data Centers · Airports & Aviation · Ports & Maritime · Telecommunications · Fortune 500 Campuses · Advanced Manufacturing · R&D Environments · Defense Facilities

Deployment Mix by Sector

Share of Nightingale deployments across critical infrastructure verticals



The security challenges across these sectors are converging. AI data centers, advanced manufacturing facilities, and high-value R&D campuses increasingly face the same operational requirements that have defined energy security for years: persistent monitoring, documented incident response, cyber-resilient architecture, and protection at a scale that human-centered approaches cannot cost-effectively deliver.

SECTION 06

Operational Proof: 440,000+ Missions

Nightingale is not a pilot program or proof of concept. We are a deployed, operational platform with a proven track record across the environments that matter most. More than 440,000 autonomous missions completed means we have encountered — and successfully navigated — the full complexity of real-world critical infrastructure operations.

440K+
Autonomous missions completed

99.7%
Mission completion rate

<30s
Average alarm verification time

Zero
Cloud dependencies in production deployments

Cumulative Autonomous Missions Completed

Nightingale fleet operations — growth trajectory

This operational experience is a strategic asset. It means our platform has been stress-tested in the field — in extreme weather, degraded networks, adversarial conditions, and regulatory audit scenarios. It means our customers aren't absorbing the risk of deploying unproven technology. They're adopting a system that has already proven itself in the environments it was designed for.

SECTION 07

Conclusion: Security That Belongs to the Infrastructure

The demands on physical security for critical infrastructure have fundamentally changed. The threat landscape is more complex. The facilities are larger and more distributed. The regulatory requirements are more specific and more enforceable. And the consequences of failure — operational, financial, regulatory, and reputational — are greater than ever.

Nightingale was built with this reality in mind. Our platform operates as part of the infrastructure itself — always on, always integrated, always capable of real-time response. We designed around the regulatory frameworks that govern our customers' environments before those frameworks were fully formed, because we believed they pointed in the right direction.

> *"We believe autonomous security should operate as part of the infrastructure itself — not as a bolt-on tool, but as a foundational layer as permanent and reliable as the facility it protects."*
>
> — Jack Wu, Founder & CEO, Nightingale Security

With more than 440,000 autonomous missions behind us and deployments across the full spectrum of critical infrastructure, we are ready to bring that capability to your environment. If you're responsible for protecting facilities where failure is not an option, we'd welcome the conversation.

Jack Wu — Founder & CEO
jack@nightingalesecurity.com