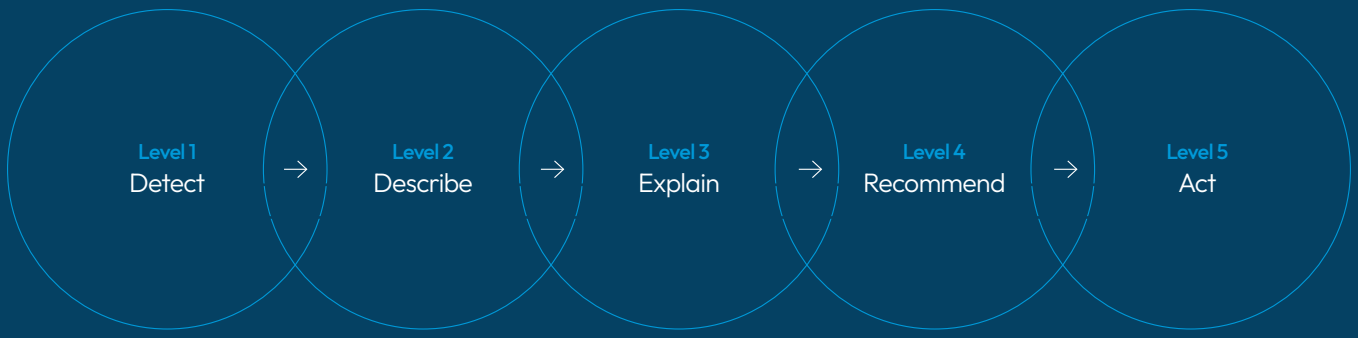
The path to intelligent security

A framework for advancing AI-enabled security operations

convergint®

At a glance

A framework for advancing AI-enabled security operations.



The situation

AI is transforming every layer of physical security technology. Most organizations have already invested in AI-enabled platforms—but few are using them to their potential. The industry has lacked a structured path for turning capability into outcome.

Where most organizations are today

Many organizations operate at Level 1 or Level 2 across most use cases. Detection and alerting are deployed. Classification exists but is rarely tuned. Cross-system correlation (Level 3) is the exception. Levels 4 and 5—forecasting and orchestrated response—remain rare.

Why it matters

The strategic returns—cost reduction, risk prevention, compliance readiness, operational scalability—do not fully materialize until Level 3 and above, and they compound significantly at Levels 4 and 5. Organizations that stop at Level 2 are optimizing a reactive model. Those that push to Level 3 and beyond are transforming security into a measurable strategic capability.

What this document provides

Part I: The framework—five levels, value curve, and the case for advancement. Part II: The strategy—priorities, compliance, data foundations, governance, system architecture, and a roadmap sequenced by impact and readiness.

The framework: five levels of intelligent security

LEVEL 1 Detect	Systems detect defined security events in real time across cameras and sensors.
LEVEL 2 Describe	Systems classify and summarize incidents with key evidence, locations, and timelines.
LEVEL 3 Explain	Systems validate incidents by correlating data across video, access control, and intrusion systems.
LEVEL 4 Recommend	Systems forecast risk patterns and device degradation and recommend prioritized interventions.
LEVEL 5 Act	Systems execute pre-approved actions.

Are you ready to lead your organization through the most significant technology shift in the history of physical security?

01 **Can you articulate your AI strategy for physical security — to your board, your CISO, and your CFO — in a way that connects capability to measurable business outcomes?**

If the answer is "not yet," you're not alone. Most security leaders are being asked about AI from every direction without a structured framework to answer. The path provides one.

02 **Do you know — by use case, by system, by site — where your organization sits today on the progression from reactive monitoring to intelligent, orchestrated response?**

Every position on the path is a valid starting point. Even the decision to retire end-of-life sensors that can't participate in an intelligent architecture is a powerful first step. The key is knowing where you are so you can plan where to go next.

03 **Are your security systems connected in ways that enable real-time correlation and validated decision-making — or are they linked through legacy integrations that still require your team to assemble the picture manually?**

There's a significant difference between legacy point-to-point integrations and a modern, interoperable architecture where systems validate each other automatically. If your team is still manually assembling the picture, the connection isn't doing the work it should.

04 **Is your organization deploying AI-enabled features with a plan for integration, governance, and lifecycle management — or are you accumulating capability without a path to outcomes?**

Capability without integration isn't intelligence — it's AI sprawl. The difference between the two is framework, governance, and a deliberate sequence.

05 **Is your organization still running security technology until it fails — or are you prioritizing investments that start the transformation to intelligent, lifecycle-managed systems?**

Every refresh decision is an opportunity to invest in systems that participate in an intelligent architecture — or to repeat a cycle that falls further behind. The organizations that treat technology refresh as a strategic moment are the ones that advance.

The path is different for every organization.
The framework for navigating it is the same.

Convergint has developed The Path to Intelligent Security to give security leaders the vocabulary, the assessment methodology, and the advancement roadmap to lead their organizations through this moment. Whether you're just beginning to assess where you stand or you're ready to build a multi-year roadmap, we're here to help.

Advancing along the path to intelligent security changes the equation.

Operational outcomes		Business outcomes
Faster response and containment	→	Lower total cost of security operations
Fewer false positives and unnecessary escalations	→	Reduced residual risk exposure
Improved operator productivity and reduced fatigue	→	Automated and defensible compliance documentation
Lower incident severity through earlier validation	→	Stronger legal and regulatory defensibility
Higher system reliability and uptime	→	Improved business continuity and operational resilience

The technology exists. The pressure is real. The opportunity is measurable.

What separates leaders from organizations constrained by legacy models is not access to AI. It is whether they have the structure, governance, and operational discipline to turn available capability into realized business outcomes.

The path to intelligent security provides that structure.

The question is: where does your organization stand, and how quickly do you intend to advance?

Scan the QR code to download the full report:

convergint