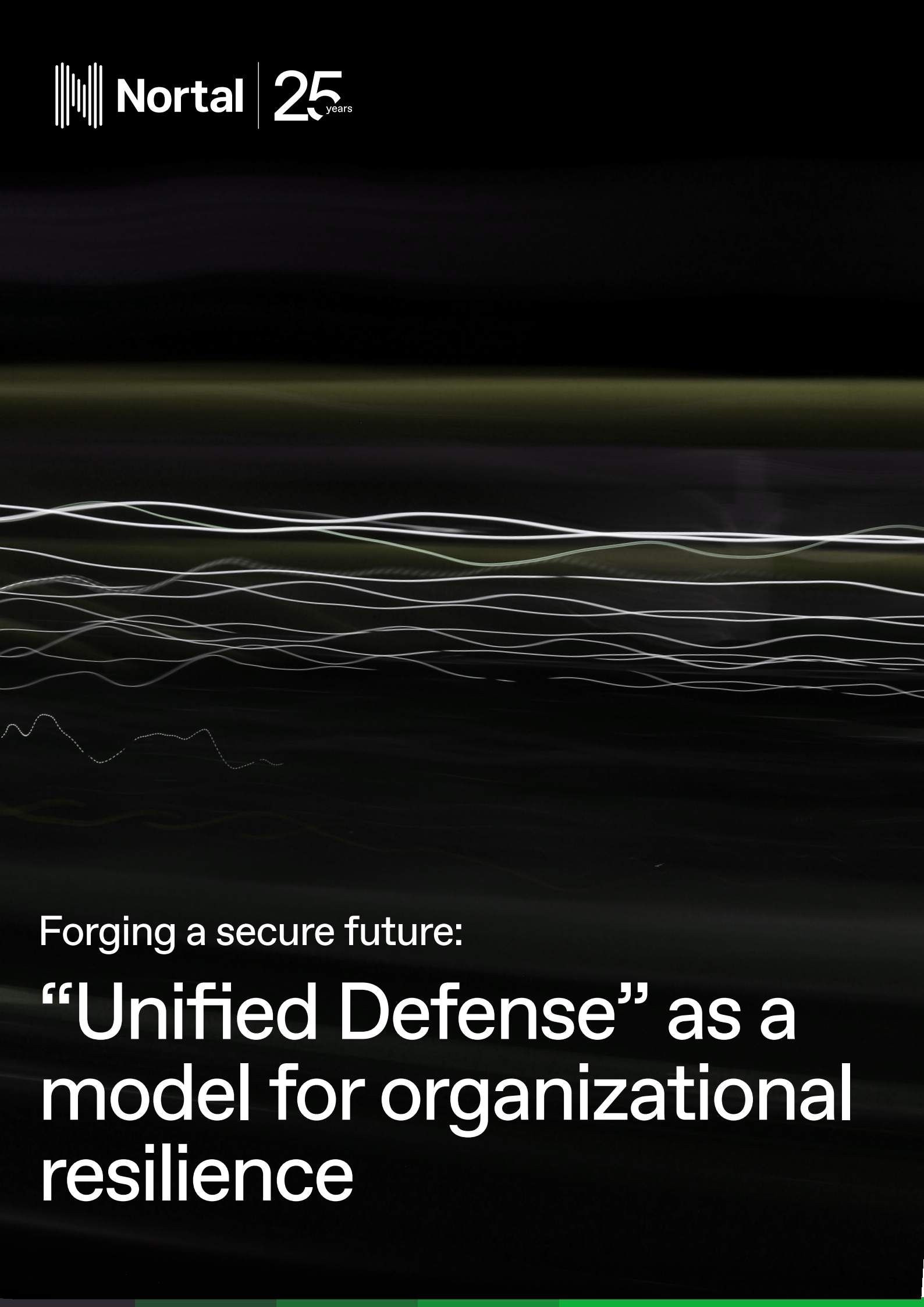
Nortal 25 years



Forging a secure future:

“Unified Defense” as a model for organizational resilience

01.

The modern battlefield: Why yesterday's security can't protect today's business

Our hyperconnected world brings many benefits to business – but it also exposes today's organizations to an ever-evolving threat landscape. In today's security battlefields, boundaries between the digital and physical realms blur and cybersecurity threats can easily transcend both.

Converged OT, IoT and IT networks and an increasingly remote workforce are just some of the factors erasing traditional boundaries between the digital and physical, creating a complex matrix of risks for organizations across the globe – opening new fronts in our ongoing security battles.

Today, a cyberattack can trigger consequences in the physical world, a physical breach can unlock digital kingdoms, and a coordinated both increases the chances of catastrophic consequences.

"Organizations that treat physical security, cybersecurity, personnel security, and operational security as separate fiefdoms are leaving gaping holes for adversaries to exploit," says James Thomas, Global Head of Cybersecurity at Nortal.

"It's time to start thinking holistically."

It's clear – traditional cybersecurity no longer fits

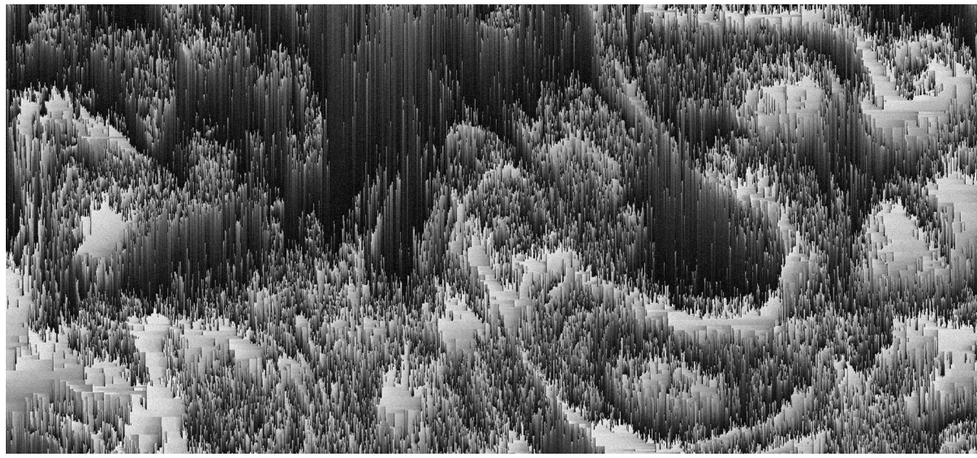
How does one respond to the modern threat landscape?

In the business world, we've seen an entire cybersecurity industry emerge in response to concerns about protecting digital assets. But too often, conventional cybersecurity programs are failing to address the new kinds of battles outlined above – and the ever-evolving vulnerabilities facing modern business.

Instead, you'll see organizations plugging their security gaps with a patchwork of systems and tools, tacking on new approaches as they enter the market and new concerns arise, but failing to think systematically.

Tools like cameras and badging systems might be deployed to protect physical assets, while firewall threat detectors are rolled out to protect digital ones. Security models like these are common, but they're also siloed, disparate and unintegrated – even as the threat landscape is not.

It's clear that an integrated, unified security approach is the way forward.



02.

Building a Unified Defense – lessons from the front line

As a starting point for rethinking security for the modern age, it may be exciting to learn there's already a proven model for a truly integrated security architecture – and it comes from an organizational sphere that's no stranger to the battlefield: the military.

Military organizations operate in high-stakes, contested environments, where mission success and survival depend equally on a deeply integrated security approach – known as "Unified Defense."

It's a strategy based on four core pillars: Operational Security, Personnel Security, Cybersecurity and Physical Security.

Operating distinctly yet together, these pillars deliver a robust, multi-domain resiliency program.

At Nortal, our deep experience supporting military and defense organizations forms the foundation of our Unified Defense service. By working alongside mission-critical teams in some of the most demanding security environments, we've refined our ability to integrate operational security, personnel security, cybersecurity and physical security into cohesive, adaptive systems.

This firsthand expertise allows us to bring proven, real-world strategies to the private sector—delivering comprehensive, scalable and resilient security solutions tailored to the unique risks facing U.S. businesses today. Unified Defense is not just a concept; it's a tested model designed to help commercial organizations anticipate threats, adapt in real time and thrive in an increasingly complex risk environment.

Why does this matter for business?

As a start, the military focuses on mission success, not unlike the way a business organization focuses on business continuity and objective achievement.

While the types of threats they face may differ, the fundamental principle of safeguarding critical data and core functions in anticipation of multifaceted threats is just as applicable to modern businesses as it is to modern defense.

Let's take a closer look at lessons from the four pillars of Unified Defense and how they might address the security challenges facing today's organizations:

The four pillars of Unified Defense

Operational Security (OpSec)

Protecting your critical processes and information

The business goal: Block adversaries from gaining insight into your sensitive operational details, strategic intentions, and vulnerabilities. Do this by identifying your “crown jewels” – the data, assets, and business functions that are critical to your success – and safeguarding them.

How it works: In an age of data leaks and social engineering, OpSec means viewing your operations through an adversary’s eyes and how they might piece together seemingly innocuous bits of information to paint a detailed picture for an attacker. Think social media, public announcements, even office layouts.

Personnel Security (PerSec)

Your people – your greatest asset and greatest risk

The business goal: Ensure individuals with access to sensitive information, critical systems, or key infrastructure are reliable, trustworthy, and understand their security responsibilities. This mitigates insider risks, whether from negligence, coercion, or malicious intent.

How it works: Your people are your first line of defense. Robust PerSec involves not just background checks, but continuous evaluation, security awareness training, and fostering a culture where security is everyone’s responsibility.

Cybersecurity (CyberSec)

Defending your digital domain

The business goal: Protect your data, networks, and information systems from cyberattack and ensure operational resilience in the face of that inevitable attack when it comes. This means securing, defending, and having the capability to respond and recover effectively, in essence, becoming resilient.

How it works: Cyberspace is a primary operational domain for every business. Strategic approaches like “Defend Forward” (proactively engaging threats) and “Persistent Engagement” (continuous vigilance) from military cybersecurity doctrine can translate to modern business as proactive threat hunting, robust incident response, and continuous defense strengthening in the commercial world.

Physical Security (PhysicalSec):

Securing your tangible assets and environments

The business goal: To safeguard personnel and prevent unauthorized physical access to equipment, facilities, materials, and documents. This protects assets against espionage, sabotage, damage, and theft.

How it works: Often overlooked in a digital-first world, a physical breach can be a gateway to devastating cyberattacks. For example, where attackers plant a rogue device or physically disable a critical OT sensor. PhysicalSec tackles this with a layered “security-in-depth” approach (Deter, Detect, Deny, Delay, Defend), shaping everything from site design and access controls to surveillance and emergency response.

03.

Our approach: Translating and optimizing Unified Defense for today's businesses

Adapting military strategy to a business landscape certainly requires a little translation. But from the front lines to corporate reality, the core logic of integrated security is the same. And in today's complex threat landscape, it's more relevant than ever to every kind of organization.

At Nortal, we believe the principles of Unified Defense can be optimized for modern business, helping organizations to enhance threat modeling, protect critical assets, streamline incident responses, and accelerate recovery.

Here's some central ideas from military strategy we believe can help organizations forge a truly adaptable and resilient security architecture:

01. Layered defense:

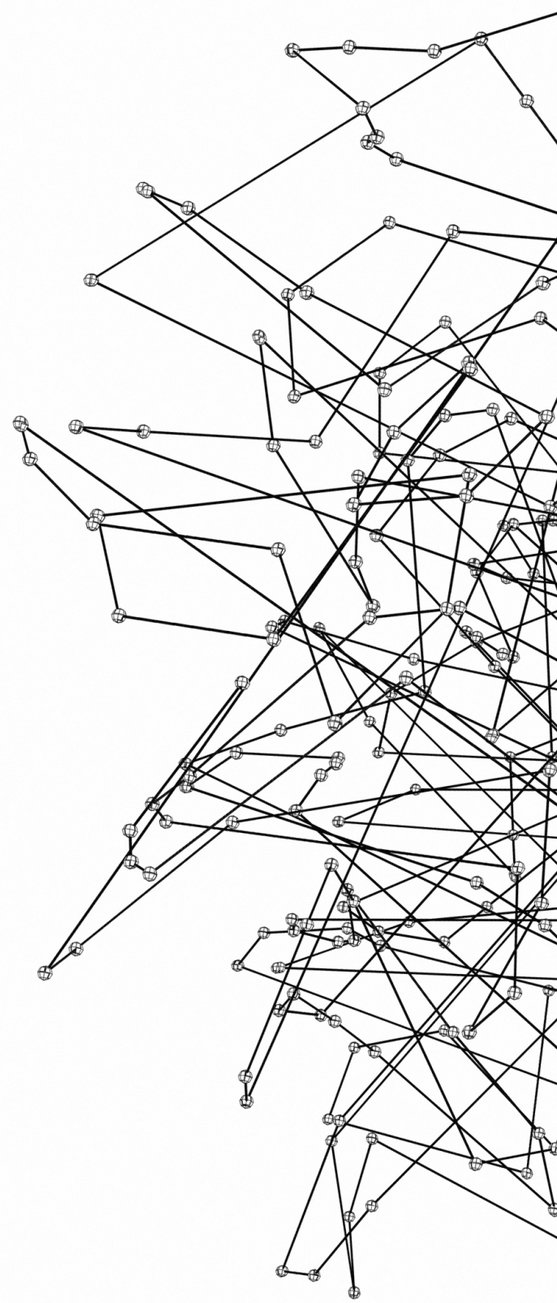
This isn't just about multiple cyber controls. It's about physical controls also protecting corporate assets. Picture a command center that's fully protected by physical barriers (PhysicalSec), personnel vetting (PerSec), network intrusion detection (CyberSec), and OpSec to conceal its operational vulnerabilities.

02. Intelligence-led security:

Understanding adversary TTPs (Tactics, Techniques, and Procedures) empowers businesses to take on proactive defense, instead of just reactive scrambling to exposed vulnerabilities. Let threat intelligence inform planning across OpSec, PerSec, CyberSec, and PhysicalSec.

03. The human element as the core:

Personnel considerations are essential for every aspect of security – a compromised or neglectful individual can undermine even the most sophisticated defenses. The military sees security as everyone's responsibility – let this concept form the basis of a new kind of security culture.



So how do the battle-tested doctrines OpSec, PerSec, CyberSec and PhysicalSec translate into tangible security measures for business when rolling out an integrated security system?

01. Unified command & control, but for business:

Just as military operations require clear command, business security needs coordinated leadership. This ensures security efforts are deconflicted, mutually supportive, and aligned with business goals. An integrated Command and Control (C2) structure, potentially under a Chief Security Officer (CSO) or equivalent, enhances the effectiveness of your overall security architecture.

02. Adopt a “mission focus” – Identify your “crown jewels”:

Just as military OpSec identifies critical information that’s vital to mission success, businesses must pinpoint their “crown jewels.” This means identifying the critical functions, processes, data, IP, systems, and personnel that would severely impact objectives if they were compromised – which is why protecting them is paramount.

03. Think like an adversary (The OpSec mindset):

Analyze your operations from an attacker’s perspective. Where are your exploitable indicators? What are your vulnerabilities? This insight is invaluable.

04. Implement layered security across domains:

Apply multiple, overlapping controls across physical, personnel, cyber, and operational domains. This looks like PerSec measures (background checks, training) complement CyberSec controls (MFA, segmentation) for personnel with physical access (PhysicalSec) to critical IT, all governed by OpSec procedures.

05. Integrate the “human domain” as a critical security layer:

Recognize employees as a vital defense line and as a potentially severe risk. Invest in PerSec (vetting, suitability), continuous security awareness training, user behavior analytics and monitoring, and cultivate a culture where security is a shared responsibility.

06. Adapt “defend forward” to a proactive industry posture:

While performing offensive cyber is rare for commercial entities, the principle of proactivity can still be applied to strengthen your security approach. This means your organization moves beyond reactive perimeter defense to active threat hunting, participation in your relevant industry Information Sharing and Analysis Centers (ISACs) for early warning, and developing robust, well-rehearsed incident response plans.

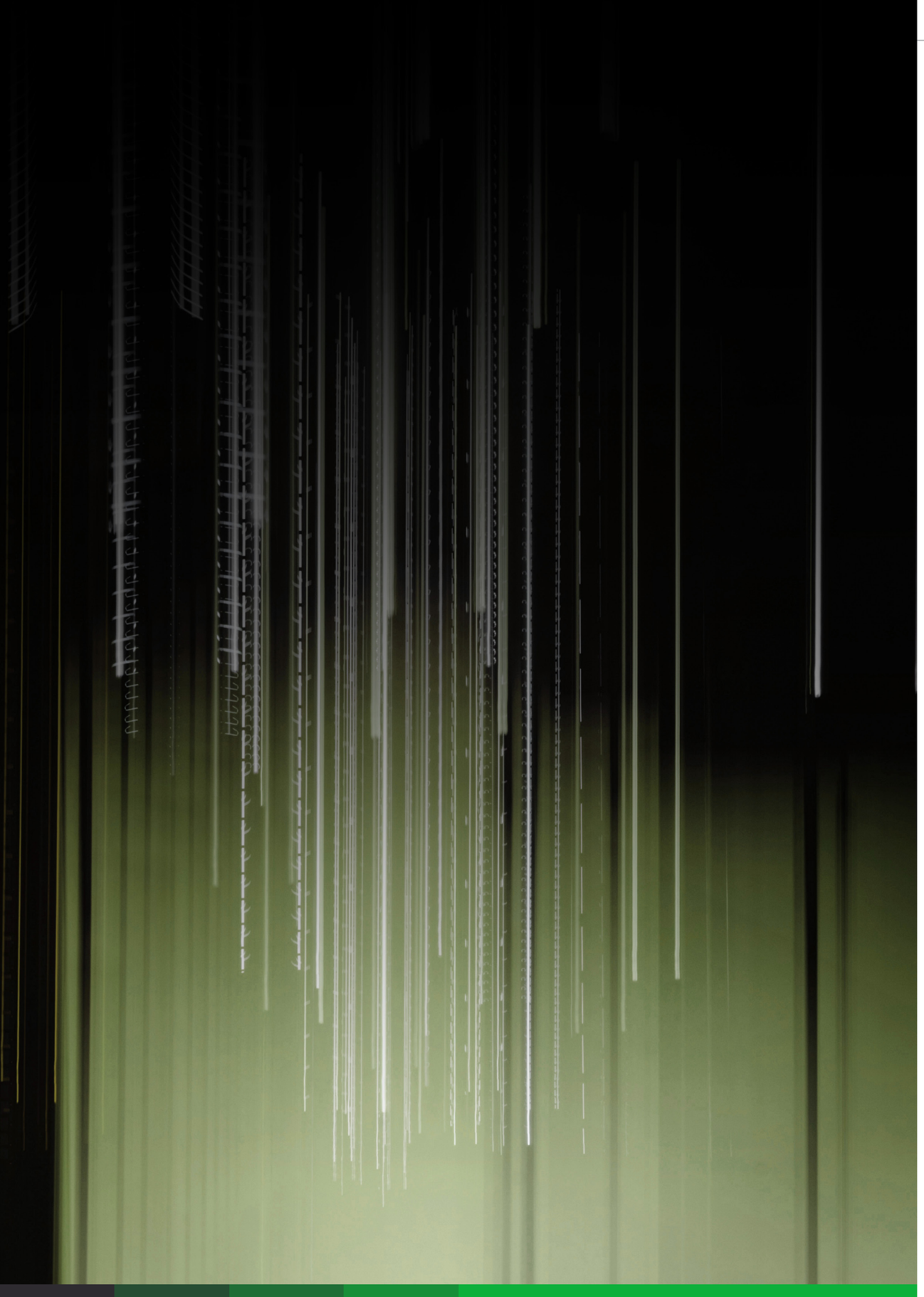
07. Risk-driven resource allocation:

Prioritize security investments based on risks to critical assets and mission objectives. Use and customize risk management frameworks to allocate budgets efficiently, focusing on mitigating the most significant threats to your “crown jewels”.

08. Don’t forget the vital role of threat intelligence

Effective threat intelligence is the glue that holds a unified defense program together. Without a shared understanding of the threat landscape across all domains, your different security domains will remain siloed and reactive. That means your intelligence must:

+ Inform all security disciplines holistically
+ Enable proactive threat hunting and vulnerability management
+ Contextualize alerts and incidents for effective response
+ Help understand adversary OpSec for counter-exploitation



04.

Our integrated security framework: Plan, implement, assure, improve

At Nortal, we've developed an adaptable and cyclical framework for rolling out and maintaining integrated security capabilities across organizations, grounded in proven Unified Defense principles to address the complexities of the modern threat landscape.

Step 1.
Plan: Laying the foundation

Objective: Establish a comprehensive, integrated security strategy and governance.

Actions: Identify “crown jewels,” conduct integrated risk assessments, define policies and governance (potentially with a unified CSO role), develop context-specific strategies, involve corporate personnel supporting OpSec, PerSec, CyberSec and PhysicalSec.

Focus: Defining protection needs across all pillars (OpSec for critical info, PerSec for high-risk roles, CyberSec for digital assets, PhysicalSec for locations).

Step 2.
Implement: Building converged capabilities

Objective: Deploy converged controls, foster security culture, and integrate security into business processes

Actions: Develop and deploy synergistic controls, foster security culture through training, establish integrated communication channels, and integrate security into business processes.

Focus: Implementing collaborative OpSec, PerSec, CyberSec and PhysicalSec procedures to protect corporate assets.

Step 3.
Assure: Verifying effectiveness & readiness

Objective: Continuously monitor, verify control effectiveness, and test readiness.

Actions: Continuous monitoring across all domains, integrated audits, multi-domain incident response drills, and measure performance (KPIs/KRIs).

Focus: Monitoring for OpSec indicators (info leakage), PerSec indicators (suspicious behavior), CyberSec indicators (threat feeds), PhysicalSec indicators (access logs).

Step 4.
Improve: Adapting & evolving security

Objective: Analyze performance trends to identify areas for improvement, incorporate lessons learned, adapt to evolving threats, and continuously enhance posture.

Actions: Analyze incidents/near misses, adapt to evolving threats/business context, incorporate lessons into Plan/Implement, refine strategies.

Focus: Operationalizing performance metrics, revising critical information lists (OpSec), updating PerSec training, prioritizing patching (CyberSec), upgrading physical systems (PhysicalSec), and improving cross-domain coordination.

The above framework is grounded in these four principles, inspired by Unified Defense strategy:

+ **Threat-Aware:** Grounded in a continuous understanding of the evolving threat landscape.
+ **Integrated & Converged:** Explicitly promotes the synergy of OpSec, PerSec, CyberSec, and PhysicalSec.
+ **Context-Specific:** Tailored to your mission, “crown jewels,” environment, and risk appetite.
+ **Continuous Improvement (The Security Cycle):** Security is iterative, not static. Adapt to new threats and lessons learned.

05.

Overcoming the hurdles: Anticipate challenges in adopting Unified Defense

Transitioning to a new, more comprehensive security architecture is not without challenges. Here's some potential hurdles to anticipate in rolling out an integrated security approach, and the solutions to overcome them:

+ **Organizational silos:** Break down traditional barriers between IT/cyber, physical security, HR (PerSec), legal, procurement and operations requires leadership commitment – potentially a CSO role or robust cross-functional, collaborative working group.
+ **Budgetary constraints & demonstrating ROI:** Justifying investment can be tough if security is seen as a cost. Demonstrate ROI through risk reduction, enhanced resilience, brand protection, loss avoidance, and reduction of cybersecurity insurance premiums and deductibles. Highlight how integrated security enables business objectives.
+ **Fostering a culture of integrated security:** This is a cultural shift. It requires continuous education, leadership messaging, interdepartmental collaboration, and embedding security into everyday processes.
+ **Managing complexity:** Start with a phased implementation focused on critical assets and significant integrated risks.
+ **Addressing the expertise gap:** Invest in cross-domain training, hire veterans with this experience, or leverage external consultants.
+ **Supply chain security:** Your security is only as strong as your weakest link. Robust third-party risk management is essential.

Resilience isn't an expense; it's an investment in your ability to operate and innovate.

06.

Conclusion: Building a secure future through Unified Defense principles

There's no doubt that the modern threat landscape demands a fundamental shift from siloed reactions to integrated, proactive defense.

When organizations lack an integrated approach, they're more vulnerable. Any adversary or attacker will always attempt to exploit the weakest points of your defense and take advantage of siloed approaches to security.

At Nortal, we believe that an integrated security model, inspired by Unified Defense and constructed with proven principles of military strategy, removes that opportunity from attackers. This makes it vital for organizational survival, continuity, and success. It's comparable to the difference between protecting yourself with a patchwork quilt or a Kevlar vest.

The goal here is not merely "security" but "enabling security" – empowering your organization to confidently pursue its objectives and thrive in a complex world.

To achieve true integrated security, organizations must:

+ Move beyond siloed thinking: Champion a holistic view across physical, cyber, personnel, and operational functions.
+ Adopt a holistic, risk-based security culture: Ingrain security as a shared responsibility, driven by risks to critical assets and objectives.
+ Invest in the integration of people, processes, and technology: True convergence requires integrated processes, shared intelligence, cross-functional collaboration, and unified technology.
+ Utilize a unified integrated security framework: The "Plan, Implement, Assure, Improve" cycle offers a practical structure to build a mature, integrated security capability.
+ Adapt technology for holistic threat assessment: AI tools unlock new possibilities for threat detection, analysis and escalation. Not every organization has trained intelligence analysts like the military does, but they can still access tools to process the threat information across their physical and digital domains, and produce actionable intelligence for risk response.

The journey to integrated security is ongoing. It requires sustained leadership, a common cross-functional collaboration focus, and a commitment to learn and adapt.

But by embracing these principles, you already begin to transform security from a cost center into a strategic enabler. This is the power to protect and the power to enable: this is true organizational resilience, battle-tested and braced for the security challenges of today and tomorrow.

Unified Defense is not just a concept—it is a proven model, ready to help commercial organizations anticipate threats, adapt in real time and thrive in an increasingly complex risk landscape.

Engage Nortal to assess your organization's full security posture. We help identify gaps, prioritize risks and align defenses across all domains—before adversaries exploit a weak link.

Connect with our security experts to take the first step toward a truly unified defense strategy.

Nortal has a proven track record of delivering comprehensive cybersecurity solutions to industries operating in complex threat environments. From AI-driven monitoring and anomaly detection to integrated network and identity data analytics, our services help organizations secure critical infrastructure, maintain operational continuity and comply with strict regulatory frameworks.

By embedding security into digital transformation efforts, Nortal enables clients to reduce risk, strengthen resilience and safeguard mission-critical assets.

We deliver tailored cybersecurity solutions aligned with national security standards and military doctrines, including integrated defense. Our programs support operational security (OpSec), personnel security (PerSec), cyber defense and physical protection through unified, intelligence-informed approaches.

Our experience includes securing defense systems, protecting classified information and developing secure digital platforms for mission planning, logistics and command operations—ensuring readiness, resilience and technological superiority in fast-changing threat landscapes.

Nortal

Get in touch

Nortal offers a national defense-level pedigree in building cyber-resilient organizations. Get in touch to detect, prevent, respond to, and recover from cyber incidents.

About the author

James Thomas, SVP Defense & Cyber in Nortal's Defense business unit. Awarded a Royal commendation for his work in Cybersecurity, James spent 21 years in the UK military as a commander and leader in the Telecommunications, Cyber and Electronic Warfare branch of the British Army.
Contact: James.Thomas@nortal.com

nortal.com

25 years of shaping the future