Cybersecurity

Nortal is a defense-proven, data-and-AI-native cybersecurity partner that designs, builds, and runs secure digital platforms for nations and mission-critical enterprises.

Core services

- Cyber Strategy & Transformation
- Governance, Risk & Compliance
- Secure Architecture & Engineering
- Data & AI Security
- Digital Trust & Privacy
- Cyber Exercises & Capability Building
- Business Continuity Management
- Security Operations Center (SOC)
- Security testing

outokumpu

Republic of Estonia
Information System Authority

Republic of Estonia
Estonian Tax and Customs Board

Ministry of Defence

ROYAL NAVY

National Cyber Security Centre

Bank of England

Our capabilities & credentials

- **Decades of experience:** Trusted by national defense, healthcare, and public sector organizations worldwide.
- **Certified experts:** Teams hold CISSP, CISM, ISO 27001 Lead Auditor, and other top industry certifications.
- **Global reach, local expertise:** Delivery across Europe, the US, and the GCC, with deep understanding of local regulations.
- **Innovation-driven:** Solutions forged in defense, battle-tested in the world's most challenging environments.

How to get started: 3 proven entry projects

1. **Critical Asset & Vulnerability Analysis:**
   Identify your most valuable digital assets, uncover vulnerabilities, and receive actionable recommendations for immediate risk reduction.
2. **Cybersecurity Maturity Assessment:**
   Evaluate your current security posture, benchmark against industry standards, and receive a prioritized roadmap for improvement.
3. **Assessment as an Exercise:**
   Test your organization's resilience and incident response plan in a real-life threat scenario that feels scarily close to the real thing.

Cyber Strategy & Transformation

Embed resilience to your business: strategy that drives operational outcomes

We align cyber programs with business goals, quantify risk, and run multi-year transformations that integrate cyber across people, processes, and technology.

Key services

- Maturity baseline
- Target-state roadmap
- Program management
- Investment prioritization
- Metrics & ROI
- Unified Defense
- SOC implementation

Our experience

UK NCSC: Strategic review using NIST CSF and actionable roadmap for a high-security collaboration platform.

Bank of England: Design, creation and establishment of a Security Operations Centre proportionate to the threats faced.

Royal Navy: Embed resilience across operations by linking cyber maturity with tangible business outcomes. Focused work on governance, risk management, cultural change, and CSOC capability development.

National Cyber Security Centre
a part of GCHQ

Bank of England

ROYAL NAVY

Why Nortal:

Business-first:
Controls translated into outcomes, ROI, and exec-level value.

Operator DNA:
Delivered mission-critical public digital services at production scale.

End-to-end ownership:
From strategy to execution, results & resilience at every stage.

Secure Architecture & Engineering

Build security into solutions: modern technology that neutralises threats

We architect and engineer secure-by-design platforms – software, cloud, data, identity, and cross-domain - so critical services stay resilient and compliant while delivering digital transformation.

Key services

- Cross-domain services
- SecDevOps
- Zero Trust design
- AI-enabled Decision Support
- Data governance
- Cloud hardening and resiliency
- Sovereign & classified cloud

Our experience

UK Ministry of Defence: Designed next-gen Data Ingest & Security Processing incldluing cross-domain and FPGA diode architecture, delivering higher throughput, lower SWaP, and significant cost savings.

UK National Cyber Security Centre: NIST CSF validated assessment and secure architecture for multinational collaboration platform, accelerating threat response, recovery, and remediation.

Global telco: Strategic cloud security modernization program, incl. Cloud Automation, IAM & Autonomous Security – to deliver a scalable, preventive, and autditable security architecture across Azure, AWS, and GCP.

Ministry of Defence

National Cyber Security Centre
a part of GCHQ

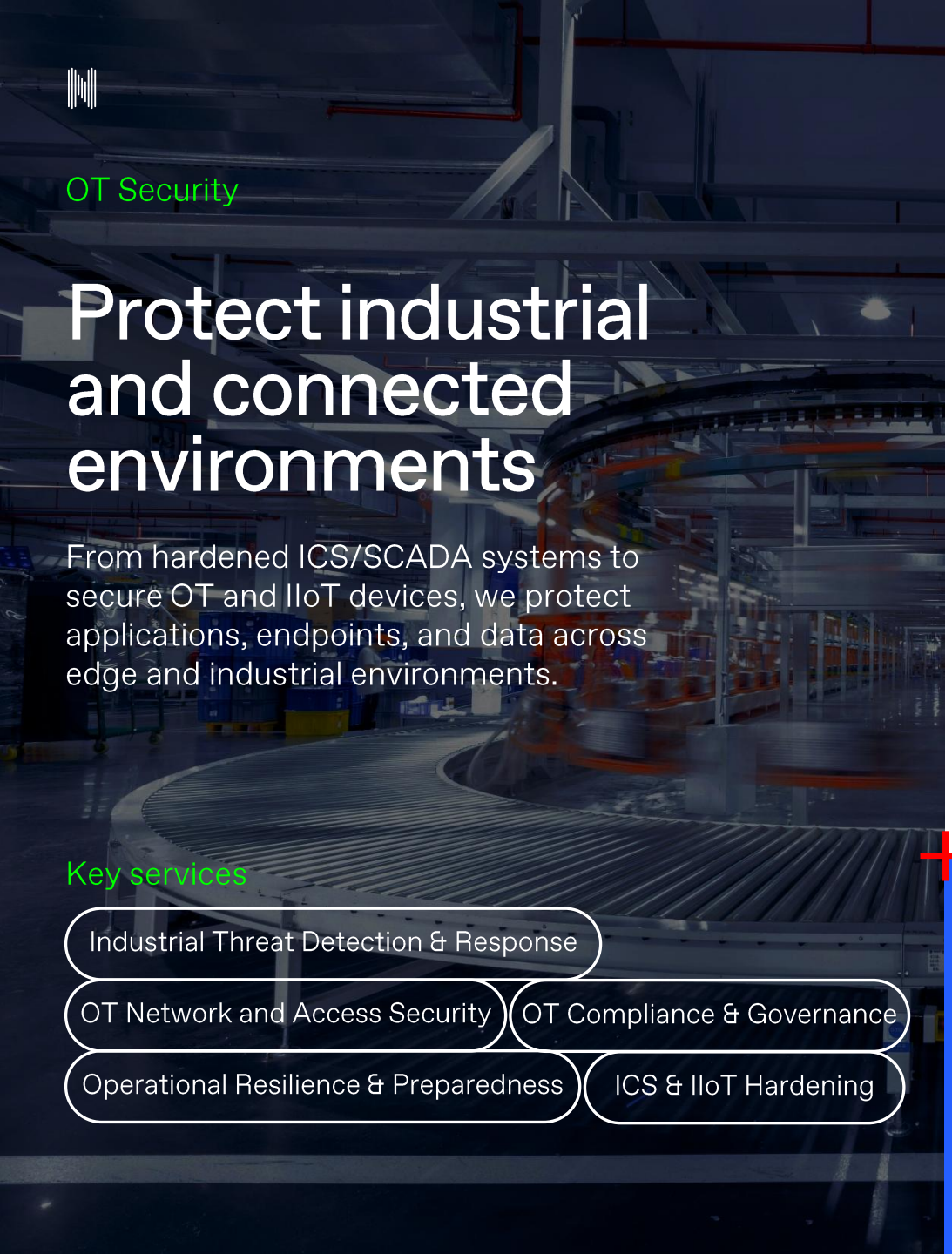
Microsoft

Why Nortal:

Defense-grade: Demonstrated architectures for classified environments, adapted for critical civilian & commercial infrastructure.

End-to-end: Our architects, engineers, & governance experts work seamlessly as one team, strategy-led delivery.

Proven patterns: Repeatable, secure-by-design blueprints speed delivery without sacrificing assurance.



OT Security

Protect industrial and connected environments

From hardened ICS/SCADA systems to secure OT and IIoT devices, we protect applications, endpoints, and data across edge and industrial environments.

Key services

- Industrial Threat Detection & Response
- OT Network and Access Security
- OT Compliance & Governance
- Operational Resilience & Preparedness
- ICS & IIoT Hardening

Our experience

Wold-class aerospace manufacturer: BCM risk analysis and BCMS implementation for regulatory compliance and resilience (ISO/IEC 27001, 22301, BSI 200-4).

SWE (water & energy): Deployed SzA attack detection in OT, refreshed ISMS, and strengthened recovery posture.

EGLV: IT/OT ISMS with KRITIS alignment and BCMS support; implemented targeted security measures in OT.

Outokumpu: Consulting on data, integration and secure hybrid-cloud strategy and architecture. Core digital services and IT networking architecture, incl. centralized Azure API Management instance to strengthen API governance and security.

Stadtwerkessen
Wir sind Zuhause.

EGLV

outokumpu

Why Nortal:

Mission-hardened: Battle-tested OT security from military-grade work, now protecting civilian infrastructure.

End-to-end fortified: Full-spectrum OT coverage – from architecture to SOC – ensuring no gaps remain.

ROI-driven: Risk-prioritized investments that turn cybersecurity spend into measurable resilience.

Cyber Exercises & Capability Building

Prepare for the real incident: build your capability and security culture.

We deliver tailored tabletop, technical, and sector-wide simulations (grounded in real threats) to develop skills, strengthen security culture, and embed resilience across business and OT.

Key services

- Tabletop exercises
- Blue/Red/Purple
- Realistic exercises
- IR plan rehearsal
- Sector war-games
- Crisis communications
- Security culture
- Capability development
- TTP run-through
- Curriculum development
- Cyberrange

Our experience

Thermo Fisher Scientific: Two custom cyber exercises engaging leadership and comms; identified improvements in lifecycle security and crisis response.

UK Civil Nuclear (Cobalt Kingfisher 2023): National-scale digital-twin exercise across 20+ orgs to validate incident response and sector coordination.

UK EFP (NATO's enhanced Forward Presence):
Cyber Fog - Custom cyber exercise, protecting CNI, ensuring local stability, mitigating cyberspace and electromagnetic threats in operational planning.

Why Nortal:

Sector realism: Digital-twin environments mirror critical processes and ICS constraints.

Leadership focus: Practice decision-making and comms, not only tooling.

Continuous learning: Findings feed directly into IR plans, policies, and training roadmaps.

Digital Identity & Privacy

Earn trust by design: privacy that enables resilience

We embed privacy-by-design, identity assurance, and data minimization into products and platforms (by using a wide range of advanced identity verification and digital identity technologies) to protect users, prove compliance, and unlock digital adoption.

Key services

- Digital Credentials
- EUDI Wallet
- Privacy by design
- Multifactor authentication
- Identity assurance
- Access management
- Digital signature

Our experience

Smart-ID: Delivered critical components enabling high-assurance eID across the Baltics, supporting secure onboarding and signing at scale.

RIA DigiDoc: Mobile digital signing that underpins trusted public e-services and verifiable transactions.

Disney: Partnered for over a decade to build the “One-ID” identity management platform – powering secure, privacy-first, and seamless user experiences across the digital ecosystem.

TxVST (German Transplant Registry, Trust Center): Implemented pseudonymization and secure data flows to safeguard sensitive health data end-to-end.

Why Nortal:

Identity lineage: Decades of eID delivery make us pragmatic about assurance and UX.

Built-in privacy: DPIA, pseudonymization, and consent operationalized into design/development.

Partner network: We know all the leading identity management providers and create the best ecosystem.

Data & AI Security

AI security and sovereignty: Safe and independent implementation of AI

We enable organizations to adopt AI responsibly by ensuring that all systems remain sovereign, transparent, and free from external influence. We secure AI systems ensuring confidentiality, integrity, and availability across the AI lifecycle.

Key services

- Risk & threat assessment
- Secure AI/ML/LLM
- Data leakage prevention
- AI sovereignty consulting
- AI compliance
- ISO27001
- ISO/IEC 42001:2023

Our experience

Estonian Air Force: AI-powered air threat identification and reporting, integrated with national defense systems.

Estonian Unemployment Fund: AI-driven risk assessment tool for unemployment services, built with secure data exchange and explainable AI.

The Lower Saxony state health office (NLGA): LLM-based solution supporting corona preparedness and crisis response for public health authorities in a security concious deployment.

Eesti Töötukassa

NLGA Niedersächsisches Landesgesundheitsamt

Why Nortal:

Secure by design: AI security embedded from architecture to operations, validated in defense and critical infrastructure.

End-to-end ownership: From risk assessment and governance to technical controls and continuous monitoring.

Full-stack AI expertise: We design, build, and secure AI solutions with our team of data scientists, delivering cutting-edge AI and security.

Governance, Risk, and Compliance (GRC)

Turn compliance into advantage: governance that builds trust

We implement pragmatic GRC – NIS2/ISO 27001 through ISMS – so you reduce risk, pass audits, and prove control effectiveness across IT and OT.

Key services

- ISMS design
- Third-party oversight
- Risk quantification
- NIS2 readiness
- Audit preparation
- ISO 27001
- KRITIS/BSIG

Our experience

EGLV (Emschergenossenschaft & Lippeverband): ISMS across IT & OT, BCMS support, and NIS2 preparation under German KRITIS context.

SWE (water & energy): Deployed industrial IPS attack detection in OT, updated ISMS, risk-based controls, and BCMS adaptation.

Wärtsilä: Reviewed cybersecurity posture against CIS v8.1, delivering gap analysis and prioritized GRC recommendations.

American Seafoods: NIST 2.0–based assessment and tailored policy development, helped safeguard critical maritime and manufacturing operations.

EGLV

Stadtwerkessen
Wir sind Zuhause.

WÄRTSILÄ

AMERICAN SEAFOODS · PRIDE OF THE SEA ·

Why Nortal:

OT + IT: Integrated and holistic approach governs both industrial and enterprise controls.

Measurable: We raise the security level through quantification, clear ROSI, and actionable KPIs – not "security on paper.

Regulatory fluency: Hands-on experience with KRITIS/BSIG, ISO 27001, BSI 200-4, and NIS2.

Business Continuity Management

Keep critical business running: whatever happens.

We build BCMS that tie critical services, dependencies, recovery priorities, and exercises into one operable plan for your time critical business processes, IT and OT, so you keep serving when incidents hit.

Key services

- BCMS design
- Impact analysis
- Service prioritization
- Crisis playbooks
- IT/OT recovery
- Wargame scenarios

Our experience

Wold-class aerospace manufacturer: Business impact and BC analysis and and BCMS implementation for regulatory compliance and resilience (ISO/IEC 27001, 22301, BSI 200-4).

EGLV: Supported BCMS and leveraged ISMS/BCM synergies for large water operations.

SWE: Crisis management optimization and alignment after OT risk assessment.

Utilities supplier (water & wastewater): Implemented reactive BCMS per BSI 200-4 framework.

EGLV

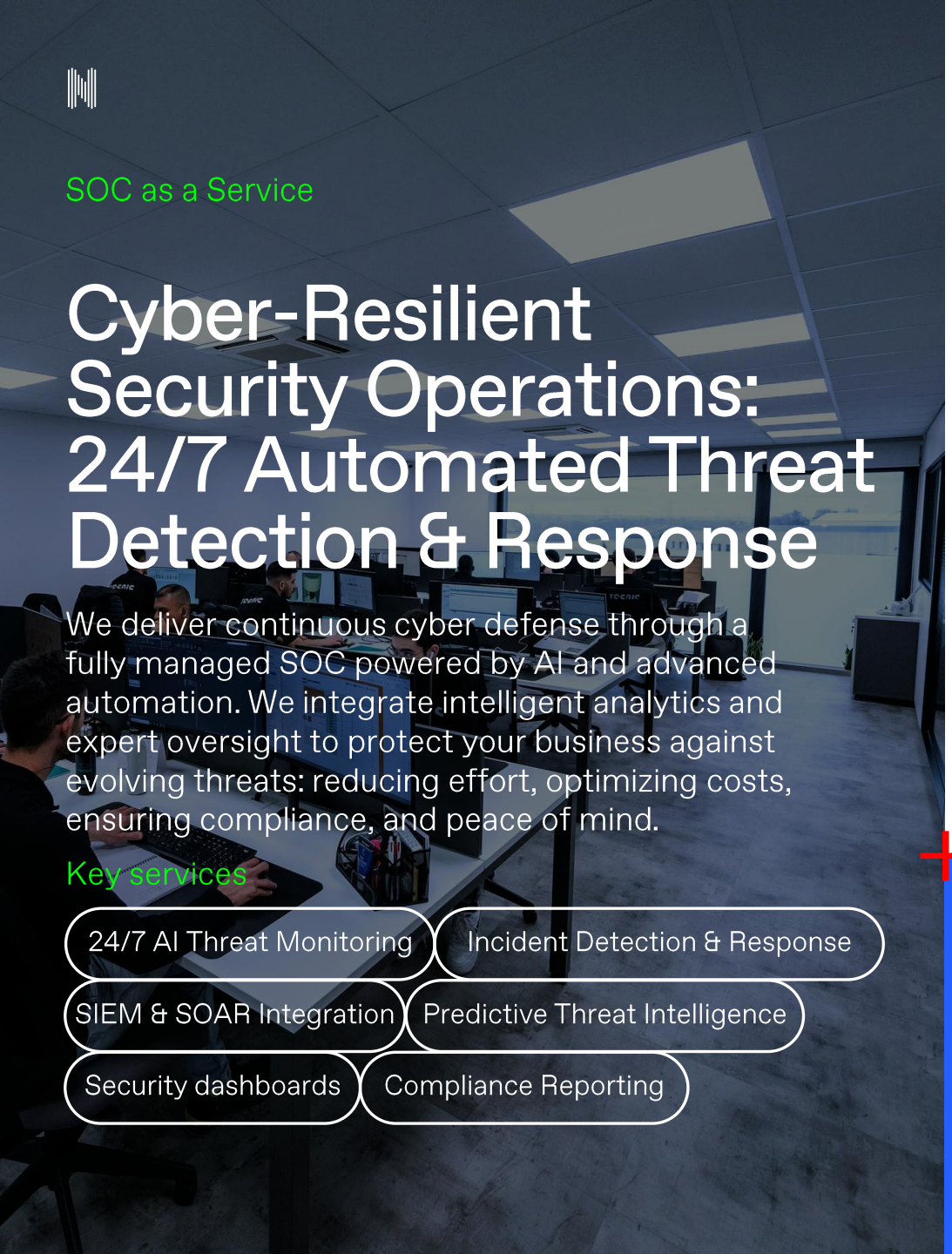
Stadtwerkessen
Wir sind Zuhause.

Why Nortal:

Critical-infra: BCM built for utilities/energy realities and regulatory obligations.

ISMS-ITSCM-OT bridge: One continuity model across plants, networks, and cloud workloads.

Tested plans: Continuity validated through exercises and incident walkthroughs.



SOC as a Service

Cyber-Resilient Security Operations: 24/7 Automated Threat Detection & Response

We deliver continuous cyber defense through a fully managed SOC powered by AI and advanced automation. We integrate intelligent analytics and expert oversight to protect your business against evolving threats: reducing effort, optimizing costs, ensuring compliance, and peace of mind.

Key services

- 24/7 AI Threat Monitoring
- Incident Detection & Response
- SIEM & SOAR Integration
- Predictive Threat Intelligence
- Security dashboards
- Compliance Reporting

Our experience

Leading provider of virtual desktop solutions: Dual-site, military-grade colocation with replication and 24/7 support - hourly backups of 54 TB, 5.5 M emails/month scanned.

Secure payment and financial technology solutions: Dedicated suite in an ISO 27001 ex-MoD facility with proactive environment monitoring/early-warning, resilient SWIFT connectivity, and immediate failover to a secondary site.

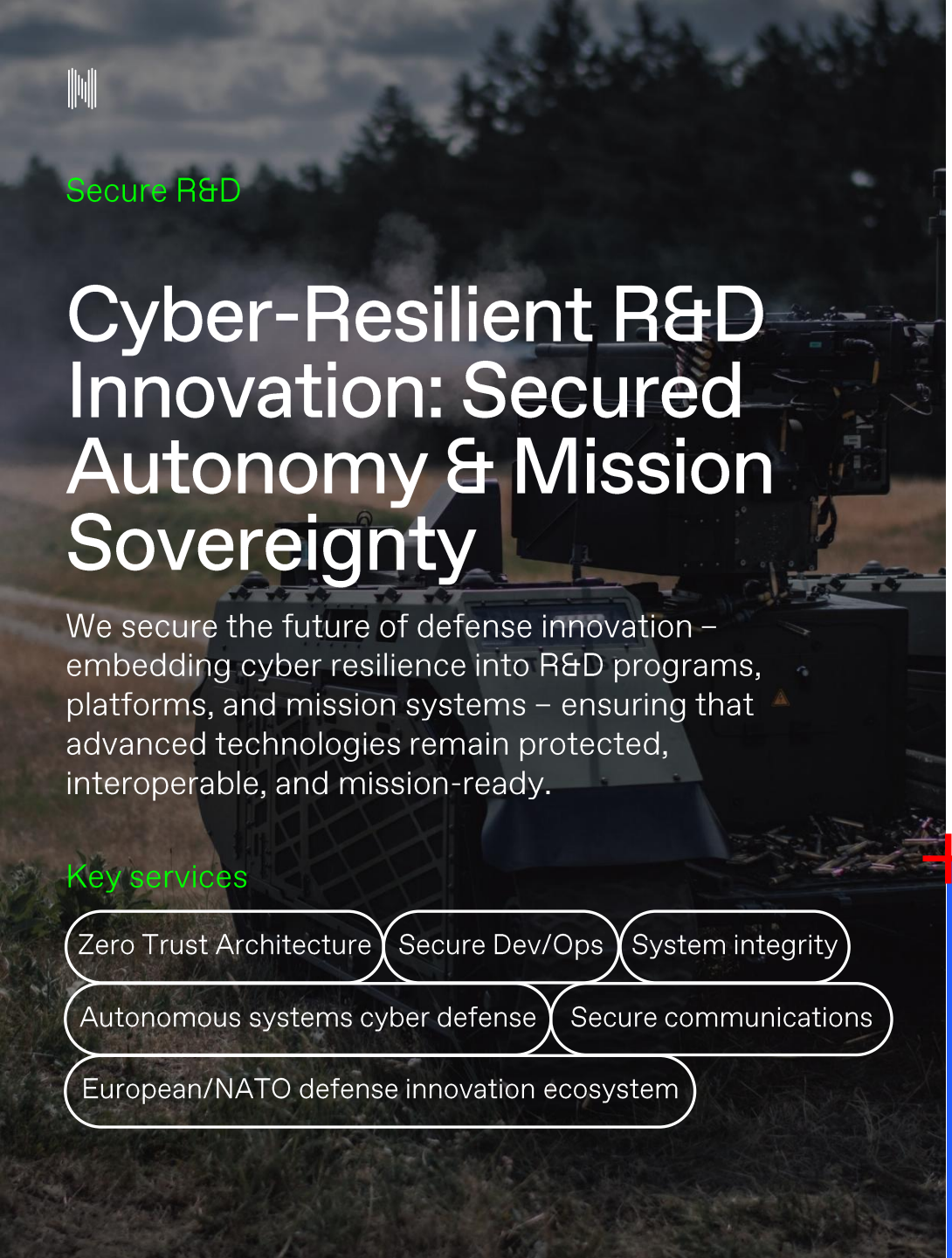
Innovator in digital security: PCI DSS-compliant, secure-cage colocation with 24/7 SOC-enabled Mastercard GVCP accreditation, accelerating time-to-market.

Why Nortal:

Outcome-driven: Continuous defense and rapid response, optimized through automation for lower operational costs.

Expert-led: Certified analysts leverage AI and advanced orchestration to maximize threat detection and speed.

Compliance assured: Automated reporting and controls streamline audits and support regulatory requirements.



Secure R&D

Cyber-Resilient R&D Innovation: Secured Autonomy & Mission Sovereignty

We secure the future of defense innovation – embedding cyber resilience into R&D programs, platforms, and mission systems – ensuring that advanced technologies remain protected, interoperable, and mission-ready.

Key services

- Zero Trust Architecture
- Secure Dev/Ops
- System integrity
- Autonomous systems cyber defense
- Secure communications
- European/NATO defense innovation ecosystem

Our experience

iMUGS & iMUGS2: Cybersecurity architecture and resilience for Europe's largest unmanned ground systems R&D, including autonomous teaming, swarming, and threat mitigation.

CITADEL Range: Development of modular, AI-enabled cyber ranges for multinational defense training and exercises. Cyber operations & mission rehearsal for EU & NATO partners.

ESC2 & EC2: Design and integration of secure, modular European command-and-control systems with advanced SecDevOps practices enabling interoperability, situational awareness, and mission execution capabilities.

EUROPEAN DEFENCE FUND
EUROPEAN UNION

NATO OTAN

REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

esa

Why Nortal:

Defense-grade expertise: Proven delivery in NATO, EU, and national R&D programs.

Trusted partner: Embedded in Europe's largest defense innovation consortia.

Mission resilience: Security engineered into every phase, from concept to deployment.