Kyūdō

SOVEREIGNTY-GRADE AI · GRC

Kyūdō Platform Overview

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · VIGILANCE BEFORE IMPACT

Governance that runs. Not governance that waits.

The martial art of Kyūdō — the way of the bow — teaches that mastery is not measured by the arrow's flight, but by the discipline that preceded it. The archer's draw, breath, and alignment determine whether the target is struck before the string is ever released.

Kyūdō, the platform, embodies the same principle. Security and compliance are not outcomes you scramble to produce. They are operating conditions you maintain continuously, so that when scrutiny arrives, readiness is already the answer.

This document is the introduction. If by the end of it you can describe what Kyūdō is, why it is structurally different from anything else on the market, and what it would change for your organization — it has done its job. Whatever comes next, deeper conversations or sharper questions, starts from here.

01 · THE GAP

Security is strong. Governance is a scramble.

Regulated organizations have invested in security platforms, including Microsoft Security. The signals are there. The telemetry is there. The tooling is there. What is missing is the layer that converts all of it into the governance artifacts your auditors, regulators, and customers will actually accept.

Legacy GRC platforms do not read your environment — they wait for evidence to be uploaded by analysts. SaaS compliance automation tools extract your posture to their cloud, creating the very sovereignty contradiction they claim to solve. Microsoft Security produces operational truth, not governed assurance. Spreadsheets do not scale to four concurrent frameworks and a quarterly board review.

The result is the same in every organization we speak to. Evidence reconstructed under deadline. Mappings done by hand the week before an audit. AI-assisted artifacts the CISO cannot defend. Risk registers that bear no relationship to the live posture they should describe. And a security team carrying both their actual job and the governance burden the GRC tools were supposed to handle.

Kyūdō was built to end the scramble — for the organizations that want to cultivate readiness before anyone asks for it.

02 · WHY KYŪDŌ

Four architectural commitments. One operating posture.

Kyūdō's differentiation is architectural, not cosmetic. Four commitments together produce a platform no other GRC tool can replicate without rebuilding from the ground up. Each commitment is a claim you can verify. None is configurable. Together, they make readiness structural.

Vector	What it means
Sovereignty-grade deployment	Kyūdō runs inside your Azure tenant — including the AI that reasons over your governance. Your data. Your identity plane. Your encryption keys. No vendor data plane, by architecture, not by promise.
Microsoft-native evidence	Defender, Sentinel, Purview, Entra, and Azure Policy signals become governed evidence automatically, in your environment, without ETL or vendor data extraction. Your security investment produces the operational truth. Kyūdō produces the audit proof.
Knowledge Graph reasoning	Controls, evidence, risks, policies, vendors, and frameworks are typed entities in a unified graph. AI reasons over the graph; every output is cited; every claim has a source. The auditor sees a graph, not a black box.
Operational AI governance	EU AI Act, ISO/IEC 42001, and NIST AI RMF built in. 114 AI governance controls. Govern the AI you deploy, using the same platform that governs your security controls. AI governance is not a separate product.

The Vanta-swap test

A useful question to ask any GRC platform: can a competitor substitute their name for the vendor's name in the marketing claim, and have the claim remain true? For most GRC platforms today, the answer is yes — the marketing is interchangeable.

For Kyūdō, swap any competitor name into ‘runs inside your Azure tenant including the AI’ or ‘114 AI governance controls’ or ‘no cross-tenant data plane by architecture’ — the claim becomes false. The architecture is the differentiator. The architecture is also the answer to every question your committee has not yet asked.

03 · THE PLATFORM

Six integrated modules. One Knowledge Graph.

Kyūdō is not a dashboard with a chatbot. It is a system of record for controls, evidence, policies, risks, vendors, and trust — connected through the Knowledge Graph, so a change in one domain propagates intelligently across the others. A new Sentinel detection rule registers as evidence under control automation, updates the risk treatment status under risk intelligence, changes a vendor's posture if the rule covers a vendor system, and updates the Trust Center's external-facing posture in real time. The integration is structural, not feature-by-feature.

Controls Hub

The authoritative registry. Controls are auto-discovered from your integrations, mapped to 80+ frameworks via Set Theory Relationship Mapping, and scored for completeness on a 0–100 scale. The single source of truth for what controls exist, what frameworks they satisfy, and how they are operating right now.

Evidence Hub

Automated collection from Microsoft Security and cloud platforms. Every artifact carries a cryptographic hash, a lineage chain back to the source signal, and an AI-computed confidence score. The auditor's ‘show me the evidence for this control’ is answered in seconds rather than days.

Policy Center

AI-authored policy grounded in the controls the policy governs. Continuous gap analysis. Citation on every draft. When a control changes, the governing policy is flagged for review automatically. Policy as a living entity, not a Word document refreshed once a year.

Risk Management

Risks linked to the controls that mitigate them and the evidence that proves the controls are operating. Posture reflects live operational reality. Board-ready dashboards present residual risk as a trajectory, not a snapshot. The conversation with the board moves from ‘what is our risk’ to ‘how is our risk changing.’

Vendor Risk Management

Automated questionnaire handling with Knowledge Graph citations. AI-scored vendor posture against 0–10 scales. Continuous monitoring of vendor public-facing posture replaces annual review. The vendor risk program operates between renewals, not at them.

Trust Center

Customer-facing transparency portal. Replaces the security questionnaire mill that consumes weeks of GRC time per quarter. Customers and prospects review your posture in a controlled portal with appropriate access scoping. Pre-fill for any remaining questionnaires with citations and confidence scores. Security reviews compress from weeks to hours.

Two engines run beneath the modules

CMCAE — the Continuous Multi-Framework Control Assessment Engine. Recalculates control completeness, capability maturity levels 1–5, and residual risk on every signal change. The mechanism that makes ‘evidence already true’ architectural rather than aspirational.

STRM — Set Theory Relationship Mapping, per NIST IR 8477. The mathematical substrate that makes one control set satisfy 70+ frameworks simultaneously. The reason Kyūdō answers SOC 2 + ISO 27001 + CMMC + HIPAA from the same evidence without redundant testing.

04 · MICROSOFT-NATIVE DEPTH

Your security investment, working twice.

Detection telemetry, identity posture, data classification, policy enforcement — your security stack already generates the operational truth about your environment. Kyūdō is the governance layer beneath it, converting those signals into audit-ready artifacts your auditors, regulators, and customers will accept. Inside your tenant. Across every framework you answer to.

Every integration is read-only, least-privilege, and authenticated via system-assigned managed identity. Nothing Kyūdō does requires admin tokens. Nothing Kyūdō does requires write access to your environment. The platform observes and converts; it never modifies.

What becomes evidence

Microsoft service	Governance role
Microsoft Defender XDR	Threat detections become control validation evidence with chain of custody.
Microsoft Defender for Cloud	CSPM findings map to controls. Drift surfaces as control regression in real time.
Microsoft Sentinel	Logging and monitoring telemetry becomes continuous evidence of control operation.
Microsoft Purview	Data classification and DLP events become data-protection evidence, automatically mapped.
Microsoft Entra ID	Identity posture and Conditional Access state feed access-control assurance.
Azure Policy	Policy evaluations become infrastructure-compliance evidence at every change.

Beyond the Microsoft stack

Microsoft is the most common deployment pattern, but Kyūdō also reads natively from non-Microsoft sources where they exist in your environment: AWS (CloudTrail, Config, Security Hub, GuardDuty); Google Cloud (Security Command Center, Cloud Audit Logs, Asset Inventory); Kubernetes (AKS, EKS, GKE, OpenShift); GitHub (Advanced Security, Audit Log, Dependabot); Oracle Cloud Infrastructure (Cloud Guard, Audit, IAM). Each follows the same read-only, least-privilege pattern.

The partner-repeatable line

For Microsoft-standardized environments, Kyūdō is the governance control plane beneath Microsoft Security. Where Microsoft Security produces operational insight, Kyūdō produces governed assurance. This is the line Microsoft sellers carry verbatim into co-sell conversations — and the line your CISO can use with the board.

05 · DEPLOYMENT

Your tenant. Your data. No exceptions.

Self-sovereignty is not a pricing tier at Kyūdō. It is the default deployment topology for regulated organizations. Two ways to run the platform; both run the same code, the same Knowledge Graph, the same modules. The difference is where the security boundary sits.

Topology	Where Kyūdō runs	When to choose it
Multi-tenant SaaS	Shared cluster managed by Kyūdō, with logical isolation per tenant. Standard SOC 2-grade SaaS deployment.	Mid-market organizations without specific data-residency mandates. Faster onboarding (provisioned in hours). Lower up-front cost. Same product capabilities.
Client-hosted Azure	Dedicated services inside your Azure tenant. Hub-and-spoke topology with strict private endpoints. AKS, Azure SQL, Azure OpenAI — all in your subscription, your tenant, your encryption keys.	Regulated organizations: defense (CMMC), healthcare (HIPAA), financial services with strict data localization, organizations with federal contracts, organizations on Azure Government / GCC High.

What sovereign deployment actually means

Four mechanisms make the client-hosted topology defensible to your security architect, your procurement team, and your auditor. None of them is configurable; they are how the deployment is built.

- No cross-tenant data plane. Every Kyūdō service runs inside your Azure subscription. There is no path for compliance data to reach vendor infrastructure, because no such path exists in the architecture.
- Private endpoints on every service. Application services, storage, Key Vault, identity, and AI inference — every service exposes private endpoints only. Traffic stays on the Microsoft backbone.

- System-assigned managed identities. Service-to-service authentication uses identities bound to your tenant. No shared secrets. No vendor-held credentials.
- Tenant-scoped AI inference. AI operations execute on Azure OpenAI in your tenant, with your model deployments, your content filtering, your audit logs.

Implementation timeline

Multi-tenant SaaS provisioning completes in hours; first sign-in same day. Client-hosted Azure deployment completes in one to two days, including Azure landing zone preparation, cluster provisioning, networking, Entra ID integration, and Sentinel connectivity. The platform is operational from Day 2; the seven priority Microsoft integrations connect across Days 3–5; the first framework activates against live posture by Day 6. Implementation is a workshop, not a procurement event.

06 · OUTCOMES

What "evidence already true" actually changes.

The architecture matters because of what it changes for the people who run governance day to day. Three concrete scenarios illustrate the operational shift. None of them is hypothetical — each is what Kyūdō customers experience within the first month of operation.

The auditor's Day 1 evidence request

An external auditor begins a SOC 2 Type II observation period and asks for evidence of access reviews for in-scope systems for the past quarter.

Conventional	With Kyūdō
GRC lead emails IT. IT pulls Entra ID Governance access review reports for the relevant systems, manually filters for in-scope users, exports to PDF, formats for the auditor. Three to five business days; multiple back-and-forth clarifications; one or two systems usually missed in the first pass.	GRC lead opens the Evidence Hub, filters by control, filters by date range. Every access review record for the period appears with hash, timestamp, lineage, and confidence score. Exported as a single PDF or shared with the auditor through the Trust Center. Same day; no IT involvement.

The customer security questionnaire

A prospect sends a 200-question security questionnaire as part of vendor due diligence. Response deadline: five business days.

Conventional	With Kyūdō
Sales engineer or GRC analyst opens the	Sales engineer or GRC analyst uploads the

Conventional	With Kyūdō
questionnaire. Manually answers each question by referencing the most recent SOC 2 report, the security policies, the BAA, and — for unanswerable questions — the GRC lead's institutional knowledge. Two to three days of dedicated effort. Quality varies by analyst.	questionnaire to the Trust Center. Kyūdō pre-fills 70–85% of answers with citations and confidence scores. The analyst reviews flagged answers, confirms or edits, exports the completed questionnaire. Two to four hours.

The board posture review

CISO presents quarterly to the board. Board wants to see security posture trajectory across the year, framework compliance posture, top risks, and material control gaps.

Conventional	With Kyūdō
CISO requests reports from security operations (Defender Secure Score), GRC (compliance status), risk (risk register), and audit (recent findings). Each team produces a slide. CISO assembles into a deck, often discovering inconsistencies that require reconciliation. Two weeks of back-and-forth.	CISO opens the Kyūdō executive dashboard. Posture clarity, control completeness, residual risk trajectory, and recent evidence trend are present in real time. Exports the relevant views directly to the board deck. The reconciliation problem does not exist because all views read from the same Knowledge Graph.

07 · WHO KYŪDŌ IS BUILT FOR

Regulated organizations on the Microsoft stack.

Kyūdō is purpose-built for regulated mid-market and enterprise organizations running Microsoft 365 and Azure. Five industries make up the core focus, each with a distinct regulatory profile and urgency.

Financial services

Banks, insurers, asset managers, credit unions, and FinTech operating under SOC 2, GLBA, NYDFS Part 500, EU DORA, and PCI DSS. Concurrent obligations are the norm. SaaS GRC platforms are increasingly disqualified from procurement on data-residency grounds. Kyūdō's client-hosted topology removes the disqualifying question.

Healthcare

Covered entities and business associates operating under HIPAA, with the pending Security Rule NPRM expected to materially raise the cybersecurity bar. ePHI residency cannot drift across vendor boundaries. Kyūdō's architecture supports the BAA chain natively because no compliance data crosses the customer's tenant boundary.

Defense and the U.S. defense industrial base

Organizations under CMMC Level 2 or Level 3 obligations, with Phase 2 enforcement beginning November 10, 2026. NIST SP 800-171 evidence collection is the highest-effort area of CMMC preparation. Kyūdō's automated evidence engine, mapped via STRM to the 110 controls of CMMC Level 2, makes the C3PAO assessment a confirmation rather than a discovery exercise.

Critical infrastructure and energy

Organizations under NERC CIP, TSA pipeline directives, EPA water-sector directives, and emerging sector-specific cybersecurity expectations. Sovereignty is doubly important: the deployment must operate inside the customer's environment, and the AI must operate there too. Manufacturing and industrial organizations with operational technology (OT) environments fall into the same operating pattern — the IT/OT boundary is increasingly inspected, and Kyūdō's continuous evidence engine surfaces drift across it in real time.

SaaS and technology

Technology organizations operating under SOC 2 + ISO 27001 + GDPR concurrently, often with SOC 2 Type II in flight while ISO 27001 recertification is in motion. The single-control-set, multi-framework operating model is the difference between a continuous program and a perpetual scramble.

08 · WHERE TO GO NEXT

Three concrete next steps.

This overview is the introduction. The conversations that follow get specific to your environment, your obligations, and your roadmap. Three paths, depending on where you are.

Architecture briefing — 30 minutes

A working session for security leaders evaluating Kyūdō. We walk the deployment in your tenant: controls, evidence flow, sovereignty model, integration boundaries. Your security architect, your GRC lead, our engineering team. The session ends with the question your committee has not yet asked, and our answer to it. Request: hello@kyudo.ai

Mission workshop — 90 minutes

A working session for GRC, audit, and compliance leaders. We map your current control set to the continuous-evidence model. The output is a documented gap list, a 90-day remediation plan against your most immediate framework obligation, and a written architecture brief tailored to your environment. Request: kyudo.ai/workshop

Trust packet — on request

A documented packet for procurement, vendor risk, and audit-committee review. Our SOC 2 attestation, architecture diagrams, data-residency statement, BAA template (for HIPAA-regulated organizations), and the Microsoft estate dependency map. Available on request.

The framework guide series

Five flagship guides cover the frameworks Kyūdō customers most commonly operate against. Each is freestanding, sourced to authoritative regulation and standards, and reflects current 2026 reality. Available at kyudo.ai/guides.

Guide	When to read it
SOC 2 Type II Preparation Guide	Before your first SOC 2 Type II observation period; for refining the existing program.
ISO 27001 Implementation Guide	Before scoping or recertifying an ISMS; covers the new-in-2022 controls and SoA mechanics.
NIST CSF v2.0 Mapping Reference	For board communication, regulator engagement, or aligning the program against a recognized framework.
CMMC Level 2 Readiness Checklist	If your organization is in the U.S. Defense Industrial Base; especially relevant given Phase 2 enforcement begins November 10, 2026.

Guide	When to read it
HIPAA Compliance Automation Guide	Healthcare covered entities and business associates; addresses both the current Security Rule and the pending NPRM.

—

The decision in front of you

The market is converging. AI features are commoditizing. Sovereignty is becoming a procurement filter, not a preference. The EU AI Act is in force. CMMC enforcement is here. Boards are asking CISOs whether their AI-assisted compliance evidence will hold up under examination.

Kyūdō was architected for the answer to be yes. The next step is a deployment workshop — a working session with your security architect, your GRC lead, and KMicro's engineering team to validate the reference architecture against your tenant, your identity model, and your sovereignty constraints. We bring the runbook and the integration scope matrix. You bring the questions your auditor will ask. That is where the conversation gets specific.

APPENDIX A · FRAMEWORKS SUPPORTED

80+ frameworks. One control set.

Kyūdō's Knowledge Graph is anchored to the Secure Controls Framework (SCF) meta-framework, with STRM crosswalk semantics per NIST IR 8477. Activate any framework below; the underlying control set populates against it without re-collection. The list reflects the frameworks most commonly activated by Kyūdō customers; the SCF coverage extends further.

Audit and assurance frameworks

- SOC 2 Trust Services Criteria (Type I and Type II)
- ISO/IEC 27001:2022 — Information security management systems
- ISO/IEC 27017 — Cloud security controls
- ISO/IEC 27018 — Cloud privacy
- HITRUST CSF
- CSA STAR Level 1 and Level 2

U.S. federal and defense

- NIST Cybersecurity Framework v2.0
- NIST SP 800-53 Revision 5.2 — Federal information systems
- NIST SP 800-171 Revision 3 — Controlled Unclassified Information
- CMMC Level 2 — 110 controls; CMMC Level 3 — 110 + 24 controls
- FedRAMP Moderate and High baselines
- CJIS Security Policy

Healthcare and life sciences

- HIPAA Security Rule (current and NPRM-anticipated)
- HIPAA Privacy Rule
- HITECH Act
- 42 CFR Part 2 (substance use disorder records)
- FDA 21 CFR Part 11 (electronic records)
- Good Clinical Practice (GCP)

Financial services

- PCI DSS v4.0.1
- GLBA Safeguards Rule (16 CFR Part 314)
- NYDFS Part 500

- EU DORA — Digital Operational Resilience Act
- SEC Cybersecurity Disclosure Rules
- SOX Section 404

Privacy and data protection

- EU GDPR
- UK GDPR
- California CCPA / CPRA
- Virginia VCDPA, Colorado CPA, Connecticut CTDPA, and other U.S. state privacy laws
- Canada PIPEDA, Quebec Law 25
- Brazil LGPD

AI governance

- EU AI Act — in force as of August 2026
- ISO/IEC 42001:2023 — AI management systems
- NIST AI Risk Management Framework (AI RMF 1.0)
- U.S. Executive Order on AI safety, security, and trustworthy development

Critical infrastructure and operational technology

- NERC CIP (electric utility)
- TSA Pipeline Security Directives
- EPA Water Sector Cybersecurity
- IEC 62443 (industrial automation)
- NIS 2 Directive (EU critical infrastructure)

Industry-specific

- FERPA (education records)
- CMMC for the Defense Industrial Base
- CSA Cloud Controls Matrix (CCM)
- AICPA Trust Services Criteria
- SWIFT CSCF (financial messaging)

Source — Kyūdō Knowledge Graph framework registry, April 2026. SCF meta-framework coverage extends further. New frameworks are added on a continuous basis through the monthly Kyūdō update channel; framework registry queries are available on request.

APPENDIX B · GLOSSARY

Terms used in this overview.

Term	Definition
AKS	Azure Kubernetes Service. The container orchestration platform Kyūdō microservices run on, in both SaaS and client-hosted deployments.
BAA	Business Associate Agreement. The HIPAA-required contract between a covered entity and any party that creates, receives, maintains, or transmits ePHI on its behalf.
CMCAE	Continuous Multi-Framework Control Assessment Engine. The Kyūdō engine that recalculates control completeness, capability maturity levels, and residual risk on every signal change.
CMMC	Cybersecurity Maturity Model Certification. The U.S. Department of Defense's cybersecurity standard for the defense industrial base, with Phase 2 enforcement beginning November 10, 2026.
Confidence score	AI-computed score on every Kyūdō output. Indicates how strongly the source signals support the conclusion. Below the human-in-the-loop threshold of 0.7, outputs are flagged for human review.
EU AI Act	European Union regulation governing the development and deployment of artificial intelligence systems, in force as of August 2026.
Knowledge Graph	The Kyūdō substrate that stores controls, evidence, policies, risks, vendors, and frameworks as typed entities with explicit relationships. The foundation that makes ‘a change in one domain propagates intelligently across the others’ architecturally true.
NIST IR 8477	Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines. The NIST Internal Report that formalizes Set Theory Relationship Mapping (STRM).
Private endpoint	Azure mechanism for service-to-service connectivity via private IP addresses on the Microsoft backbone, never traversing the public internet. The default Kyūdō client-hosted networking pattern.
SCF	Secure Controls Framework. The meta-framework substrate that anchors the Kyūdō Knowledge Graph; over 1,470 controls across 80+ frameworks.
STRM	Set Theory Relationship Mapping (per NIST IR 8477). The

Term	Definition
	mathematical substrate that makes one Kyūdō control set satisfy 70+ frameworks simultaneously.
Tenant	In Azure terminology, an Entra ID-bounded directory representing your organization. In Kyūdō terminology, your isolated data and configuration boundary within the platform.
Trust Center	The Kyūdō module that provides external-facing posture visibility for customers, partners, and regulators.
Zanshin	The state of unbroken awareness in the martial art of Kyūdō. The philosophical anchor for the platform: continuous readiness as a condition of operation, not an event.