Indigo Vault White Paper

Title: Next Generation Document Security Built for Compliance and AI Resistance

Subheader: Regulatory burdens and AI vulnerabilities leave documents at risk

Industry Trends

In the age of AI and escalating security threats, data protection and security garner a lot of attention. But there is a lesser known and equally at-risk area of the enterprise that attracts less attention: document protection. Enterprises are facing a convergence of risks that make document protection more urgent than ever.

€5.7B Noncompliance fines issued by EU regulators in 2024.
Source: CMS Law

2.7x Additional cost organizations pay when they fail to enforce strong compliance frameworks, compared to the cost of maintaining frameworks.
Source: Help Net Security

83% Of organizations reported at least one insider leak in 2024.
Source: Cybersecurity Insiders

$72B Expected revenue from quantum computing in 2035, from $4B in 2024.
Source: McKinsey

Compliance and board-level risk is rising. Enterprises today are wrestling with an unprecedented regulatory burden and boards are treating document security as a material, actionable risk. In the EU for example, GDPR enforcement is intensifying. By March 1, 2025, EU regulators issued approximately €5.7 billion in fines across roughly 2,245 cases. In addition to growth in the number of fines, the average cost of a GDPR fine jumped 30% in 2024 to €2.8 million. Organizations that fail to enforce strong compliance frameworks face costs that are 2.7 times higher than maintaining them, through fines, breach fallout, business disruption, and lost productivity.

Additionally, new regulations increase compliance burdens. Legislation such as the EU's NIS2, DORA, and the NERC CIP standards in infrastructure now demand more rigorous cyber risk preparedness and third-party oversight. Finally, board oversight is evolving. In 2024, generative AI, data transformation, and rising cyber threats landed on boardroom agendas. And expectation for proactive risk governance continues to rise.

Regulations impacting document governance

- Finance: EU's DORA enforces ICT resilience and audit-ready documentation.
- Critical infrastructure: New NERC CIP standards stress encrypted protection of system design docs.
- Healthcare: HHS Cybersecurity Performance Goals and proposed HIPAA updates call for encryption and stronger risk analysis.
- Cross-sector*:* NIS2 and the EU AI Act expand reporting, governance, and data residency obligations.

With the rise of compliance challenges globally, at the document-level, **document threats are intensifying, especially from the newest threat frontier: AI**. Despite the benefits, generative AI presents a major security challenge to enterprises, from both AI scraping — when AI systems ingest sensitive documents that were not properly protected —

and AI leakage — when employees paste sensitive information unknowingly into AI models. Once inside an AI system, data is irretrievable and often indefensible in court.

Additionally, sensitive documents are increasingly targeted by insiders and malware. Insider-driven leaks are rising, with 83% of organizations reporting at least one leak in 2024, and over 50% of organizations more than six. The sophistication and intensity of malware attacks is also growing with 146% more ransomware attacks this year than 2024, with manufacturing, technology, and healthcare being the most-targeted industries. The oil and gas sector saw a spike in ransomware attacks of 900% since last year.

Finally, quantum computing is moving from development to deployment, which presents an additional challenge to document security. The sector is expected to grow from $4 billion in 2024 to $72 billion in revenue in 2035. Adversaries are harvesting encrypted files today with the intent to decrypt them later. This "harvest now, decrypt later" threat puts enterprises' intellectual property and sensitive data at risk.

Why Conventional DLP, IRM, and Cloud-Native Vaults Fail

For years, enterprises have relied on Data Loss Prevention (DLP) and Information Rights Management (IRM) to secure sensitive information. But in today's threat landscape, where AI, quantum, and insider risks converge, these legacy approaches leave dangerous gaps in security.

DLP stops at the perimeter and cloud-native vaults don't close the gap. Traditional DLP tools are designed to detect and block data exfiltration events, but once a document is opened, that protection ends. Sensitive content can be copied, screenshotted, or pasted into an AI tool without detection, making DLP ineffective against today's insider-driven leaks and AI-enabled risks. Meanwhile, cloud-native vaults claim continuous protection but typically rely on storage-level encryption alone, offering no defense once files are in use.

IRM breaks down in real-world workflows, just like many SaaS vendor "policy wrappers" do. IRM solutions attempt to enforce rights by wrapping documents with policy-based restrictions. But they are brittle and intrusive: they often fail when files move across platforms, are shared externally, or need to be used offline. Users bypass them for productivity, leaving enterprises exposed. Similarly, vendor-specific controls often collapse when documents leave their native ecosystem—undermining cross-border collaboration and compliance.

Neither DLP, IRM, nor cloud-native security vendors were built for AI or quantum. These tools predate the AI revolution and the coming quantum era. They offer no defense against AI scraping, no safeguards against employees pasting sensitive content into LLMs, and no ability to withstand "harvest now, decrypt later" quantum attacks. At best, they were built for yesterday's threats, not today's or tomorrow's.

> "With many companies adopting AI systems, they're now at risk of inadvertent internal data leaks, as AI scans their system to learn their company data set and can inadvertently add confidential data to public documents. While technological advancement is a positive for business, security needs to keep pace to protect intangible assets, whether that be confidential client information, financial trading formulas, business strategies or legal documents."
> **- Sean Plankey** | Global Leader of Cybersecurity Software at WTW

All share the same compliance and governance blind spots. DLP, IRM, and most cloud-native vaults operate at the data level, not at the document level. As a result, they can't enforce jurisdictional residency mandates, continuously align with frameworks like NIST or ISO, or provide board-level visibility into document-specific risks.

Enterprises that continue to rely on DLP or IRM, or storage-focused vaults for security are discovering that these traditional tools fail to protect the one thing adversaries target most directly: the document itself.

How Indigo Vault Redefines Document Protection

In response to the converging pressures of compliance, AI, and quantum, WTW created Indigo Vault Docs. Tested by over 8,000 professionals internally, Indigo Vault Docs is a zero-trust vault to protect sensitive documents from regulatory exposure, AI vulnerabilities, insider threats, and quantum risk, with its always on encryption – at rest, in transit, and in use.

Indigo Vault delivers:

- **Risk-aligned compliance by design:** Built-in, document-level controls and audit telemetry enforce data residency mandates automatically, with geo-fenced protections and verifiable residency attestations that prove where documents are stored and accessed. This keeps enterprises audit-ready across borders and allows Chief Risk and Compliance Officers to demonstrate compliance continuously.
- **AI-resistant, zero trust document vaulting:** Every file is encrypted and access-controlled continuously, even when open, shielding against insider misuse, scraping, and unauthorized access. Indigo Vault Docs provides AI-proof guardrails, not just encrypted storage, ensuring sensitive content stays protected even in AI-driven workflows.
- **Post-quantum encryption:** Files are protected with U.S National Institute for Standards & Technology (NIST)-compliant future-proof cryptography, eliminating the "harvest now, decrypt later" vulnerability. Indigo Vault Docs also aligns with PQC standards and applies future-proof key rotation, ensuring sensitive data remains secure for decades to come.

- **Seamless user experience:** Integration with Microsoft corporate environment ensures protection is embedded, not bolted on, so users remain productive while documents remain secure.

Four Use Cases at The Frontier of Data Protection

With use cases in compliance, residency, AI, and quantum, Indigo Vault Docs delivers unique protection where conventional tools fail.

Challenge: Increasing regulatory burdens and board-level mandates	**Solution: Indigo Vault risk-aligned compliance** CISOs struggle to align document security with board-level risk tolerance and compliance mandates. Regulators now expect continuous proof of control effectiveness, while boards demand assurance that sensitive documents are governed with the same rigor as financial data or operational risk. Indigo Vault Docs embeds governance directly into document workflows, delivering verifiable compliance attestation that competitors lack. Access controls are enforced consistently at the document level across users, geographies, and workflows, while real-time telemetry is automatically mapped to standards such as NIST CSF, ISO 27001, and emerging AI governance frameworks. This makes audits both straightforward and defensible. At the same time, governance teams gain board-ready visibility—quantifying risk reduction, detecting anomalous behavior, and presenting compliance evidence that builds trust with executives, regulators, and auditors alike. With Indigo Vault Docs, enterprises move beyond static policies to living, auditable governance, ensuring documents remain compliant and trusted in an era of escalating regulatory scrutiny.

Challenge: Proving and enforcing data residency	**Solution: Indigo Vault sovereignty & data residency** Governments and regulators increasingly require that sensitive data be stored and processed within national borders under frameworks such as GDPR, DORA, HIPAA, and MEA localization laws. This creates operational and compliance friction for enterprises relying on global cloud platforms that lack native jurisdiction enforcement and cannot prove compliance in an audit. Indigo Vault Docs eliminates this risk by providing automatic residency enforcement and auditable attestations that demonstrate where documents are stored and accessed at all times. With built-in data location controls, ready-to-go audit logs, and attestations mapped to regulatory frameworks, Indigo Vault Docs keeps enterprises compliant and audit-ready—capabilities conventional solutions cannot deliver.

Challenge: AI leakage	**Solution: Indigo Vault AI-resistant document vaulting**

and scraping	Enterprise data is at risk from LLMs, plugins, and embedded AI assistants. Once exposed to an AI model, sensitive data may be irretrievable and indefensible in court. Indigo Vault Docs goes beyond blocking and containment by embedding AI-resistant protections at the document level**:** • AI-invisible zones**:** Sensitive documents remain encrypted and inaccessible to AI tools, preventing scraping or leakage. • Context-aware encryption: Encryption policies adapt to document type, sensitivity, and jurisdiction, ensuring protections are enforced continuously—even when files are in use. • Adversarial detection**:** Behavioral analytics identify anomalous attempts to exfiltrate or expose sensitive content, including misuse of AI interfaces, and trigger automated safeguards. • Guardrails for safe AI adoption: Rather than banning AI, Indigo Vault Docs enables enterprises to define human-only access zones, enforce redaction policies, and provide audit trails that keep AI use compliant and aligned with governance frameworks. As a result, enterprises can embrace AI productivity while ensuring that sensitive content stays out of AI reach and regulatory obligations remain intact.

Challenge: Harvest now, decrypt later	**Solution: Indigo Vault post-quantum encryption** Data that must remain confidential for decades, such as intellectual property, legal records, or health information, is already at risk from adversaries harvesting encrypted files today with the intent to decrypt them once quantum computing matures. This "store-now, decrypt-later" tactic creates an invisible but mounting liability that boards and regulators increasingly recognize as a critical compliance issue. Indigo Vault Docs addresses this challenge with a future-looking security model**:** • NIST PQC standards: Files are encrypted using algorithms aligned with the U.S. National Institute of Standards and Technology's post-quantum cryptography standards, ensuring resilience against emerging quantum capabilities. • Legacy file protection: Sensitive archives can be re-wrapped with PQC encryption, eliminating exposure in older, pre-quantum formats. • Board-level compliance: Indigo Vault ties quantum-ready encryption directly to enterprise risk frameworks, giving Chief Compliance Officers and boards the assurance that long-lived data is protected not just today, but against tomorrow's threats.

	With Indigo Vault, enterprises gain a future-proofed compliance posture, eliminating quantum risk while demonstrating proactive governance to regulators and stakeholders.

Extending WTW's Risk Leadership into Document Security

WTW is a global professional services company, providing data-driven solutions in the areas of risk, people, and capital. We make organizations more resilient, workforces more motivated, and help clients maximize performance. Indigo Vault Docs is the culmination of WTW's two centuries of risk management expertise, now extended to the most overlooked risk surface — the document.

We have expertise in:

- **Cyber insurance and risk scoring:** WTW helps thousands of clients manage and insure against cyber risk. By reducing document vulnerabilities, Indigo Vault Docs directly improves clients' overall security posture and can help lower cyber insurance costs.
- **Timing market needs:** With quantum threats approaching, there is a narrow window for enterprises to future-proof their document security. WTW's focus is on transforming tomorrow, staying a step ahead of quantum's impact on your enterprise and delivering solutions that protect you both now and in the future.
- **Proven in-house deployment:** Indigo Vault Docs has already been implemented by WTW's own 8,000 professionals, making this a proven solution.

Future-Proofing Your Enterprise

The escalating complexity of regulatory mandates, coupled with rising board-level scrutiny, has made document protection a compliance imperative. Yet conventional approaches leave dangerous gaps in security. Indigo Vault Docs closes those gaps by embedding risk-aligned compliance directly into document-level controls, telemetry, and verifiable audit trails, enabling enterprises to continuously demonstrate adherence to frameworks such as NIST CSF, ISO 27001, and AI governance standards.

Indigo Vault Docs also enforces AI-resistant vaulting to prevent leakage, scraping, and unauthorized LLM access, while providing post-quantum cryptography that mitigates 'harvest-now, decrypt-later' attacks. Combined with geo-fenced residency attestations and verifiable compliance evidence, Indigo Vault Docs ensures board-level trust and regulatory readiness for the documents that matter most.

Engage with Indigo Vault today:

⇒ **Ensure your directors understand AI and quantum risk readiness.**
⇒ **See a sovereignty attestation in action.**
⇒ **Be one of the first five regulated enterprises to validate AI-proof document vaulting.**

Prepared by C&Z Marketing
smeade@candzmarketing.com
www.candzmarketing.com