Security begins at backup.
We deliver immunity by design.

Investor Whitepaper

Valutis TECHNOLOGIES

GARDIEL

Pure Protection. Zero Compromise.

Executive Summary

With Gardiel, Valutis Technologies is building a security architecture for a time when traditional backup concepts are no longer enough. As ransomware increasingly targets not only production systems but backup environments as well, that layer becomes the point where business continuity is either preserved or brought to an expensive halt.

The consequences go far beyond IT disruption. They affect availability, operations, delivery capability, trust, auditability, and in extreme cases the financial stability of an organization. Recovery has therefore become a business-critical capability.

Gardiel closes that gap. The system protects data at write time, keeps it fully available for recovery, and creates the basis for controlled, verifiable recovery. Rather than treating backup as a passive safeguard, Gardiel turns the backup environment into an active protection layer.

For organizations, that means stronger protection, less operational friction, and a restart that is grounded in architecture rather than hope. For investors, Gardiel is more than a cybersecurity product. It is the foundation for a new reference standard in trustworthy data resilience.

The Reality of Ransomware

Ransomware is no longer an isolated IT risk. It is one of the strongest drivers of cyber loss and cyber insurance exposure, with attack frequency, sophistication, and financial impact continuing to rise. Attackers now target not only production systems but backups as well, because that is where the outcome of recovery is decided.

Independent market outlooks estimate annual victim costs at more than €245 billion by the start of the next decade. For organizations, that means production downtime, delivery disruption, reputational damage, regulatory pressure, and rising expectations from insurers and auditors.

That shifts the real question. It is no longer only about whether an attack can be prevented. It is about how quickly and how cleanly an organization can return to operation after an incident. Recovery is no longer just an IT task. It is a management, risk, and board-level issue.

The Solution

Gardiel is installed between the corporate network and the backup infrastructure, where it introduces a new security logic. As a hardware-anchored gateway with a unidirectional data diode, it protects data at write time and turns the backup environment into an active protection layer.

Data remains fully available for recovery, while injected malware can no longer execute in that state. Protection is therefore not added later as a secondary control. It is built directly into the write path.

A key advantage is that Gardiel does not replace existing backup environments. It strengthens them. Organizations can continue to use their current processes, systems, and investments while adding exactly the layer that matters most when incidents occur.

How Gardiel Works

Gardiel follows a clear sequence of backup, forensics, and recovery.

During backup, data enters the protected storage environment exclusively through the unidirectional data diode. At write time, it is protected in real time using an instance-specific obfuscation unique to each Gardiel deployment. It remains fully available for recovery, while malware can no longer execute in its obfuscated state.

For forensics and remediation, the entire backup environment remains continuously inspectable, even while obfuscated. A fully isolated administrative network supports monitoring, analysis, and targeted remediation. Access is secured by a hardware key. Signatures, YARA rules, and other threat indicators can be applied at any time, including to older snapshots. This makes it possible to identify, verify, and remove malicious components without allowing embedded malware to become active.

When data is needed from backup, the data path is switched in a controlled manner into recovery mode using a separate physical hardware key. At that point, only the direction back into the corporate network is active. During transfer, the data is transformed back and immediately becomes available again in its original, readable form. Recovery becomes a controlled and repeatable process.

Why Gardiel Is Different

Gardiel combines several characteristics that are unique in this combination. The unidirectional data diode prevents any return path into the production network. Instance-specific obfuscation protects data states at write time. The obfuscated backup environment remains continuously inspectable. Forensics and remediation run in an isolated administrative network. Recovery is controlled and strictly one-way.

Together, these elements create a level of protection that captures the security effect of classic air-gap models without their operational drawbacks. Gardiel delivers air-gap-grade security at operational speed and complements existing backup environments instead of replacing them.

The difference from software-only approaches lies above all in the timing and the nature of protection. Gardiel does not step in only after an incident has been analyzed or a restore has been prepared. Protection is built into the data flow itself. The backup environment remains available, inspectable, and ready for recovery.

Technological Foundation and Proof Points

Gardiel is built on a credible technological foundation. That foundation includes more than 350 patent claims across four patent families, along with hardware-validated proof of functionality. Gardiel is therefore not just intellectual property on paper. It is a technically realized and verifiable hardware-based system.

That foundation is reinforced by a clear product logic, investor-ready communications, and an architecture that is already aligned with real market needs. For auditors, insurers, partners, and prospective pilot customers, this creates a significantly higher level of credibility than purely theoretical or software-only concepts.

For investors, that translates into defensibility, pricing power, and stronger conditions for certification, diligence, and market entry.

Customer Impact

In a crisis, organizations need more than stored data. They need states that are available, inspectable, and cleanly recoverable. That is the core customer value of Gardiel.

The architecture prevents compromised backups from becoming the bottleneck of recovery. It creates a continuously verifiable backup environment, reduces reliance on manual air-gap processes, and makes recovery predictable. That shortens downtime, lowers operational complexity, and strengthens confidence in an organization’s ability to restart.

This is especially relevant in regulated and mission-critical environments. Wherever availability, integrity, and verifiability are required at the same time, Gardiel provides a technical answer to that exact combination.

Target Market

The initial focus is on larger midsize organizations with distributed IT and OT structures, lean security teams, and a strong need for tamper-resistant backups and rapid recovery. In these environments, the pressure to remain both secure and operational is especially high.

From there, the path extends into regulated and mission-critical segments such as healthcare, manufacturing, the public sector, and sovereign cloud environments. These markets combine high requirements for availability, auditability, and resilience with the need to continue operating existing system landscapes.

Business Model

Gardiel is offered as Hardware-as-a-Service, creating the basis for predictable recurring revenue. The model combines hardware, maintenance, and updates with a clear expansion path through additional units, forensic services, premium SLAs, and training.

From an investor perspective, this model is attractive because it is not built on one-time product sales. It is built on recurring revenue, clear packaging, and expansion potential by site and customer size. In a market defined by urgency and relevance, that creates a strong commercial logic.

Patent Strategy

The patent portfolio protects the core methodology, while the architecture deliberately relies on standardized hardware combined with a proprietary process. That creates a balance of broad protection and practical implementation.

The current portfolio structure also provides flexibility through divisional filings and future strategic expansion. For investors, that matters because it strengthens technical differentiation, defensibility, and scalability at the same time.

Next Development Steps

The next steps focus on finalizing the hardware, initiating certification, launching initial pilot projects, and preparing a structured market entry in Germany. Over time, the roadmap extends to cluster failover, auto-restore, formal certifications, and vertical expansion into regulated industries.

Long term, Gardiel's vision evolves toward a managed resilience network with telemetry, intelligent anomaly detection, and tighter alignment with insurers, auditors, and governance processes.

Funding Ask

Valutis is currently raising €1.5 million for an 18-month runway. The capital will be used to finalize the hardware, start certification, execute ten to fifteen pilot projects, and prepare for market launch in Germany.

Based on the current plan, the funds will be allocated across research and development, hardware and staffing, patent internationalization, certification and forensic tooling, as well as marketing and sales. In parallel, targeted introductions to banks, insurers, and critical infrastructure partners remain strategically important.

Team

Behind Valutis is a team that brings together technology development, cybersecurity, intellectual property, and entrepreneurial execution. That combination matters because Gardiel must prove itself not only as an idea, but as a real product, a credible security architecture, and an investable market proposition.

The team is further strengthened by capabilities in product design, brand development, and marketing, ensuring that technology, product experience, and go-to-market are aligned in the next phase. Together with experienced voices from technology and storage-related environments, this creates a setup in which product, compliance, market presence, and scaling are closely coordinated.

Investment Invitation

With Gardiel, Valutis is building a new reference standard for trustworthy data resilience. If recovery must become provable, fast, and anchored in hardware, now is the moment to help shape that category.

An investment in Gardiel accelerates certification, pilot projects, and market entry. More importantly, it supports the development of a security architecture that no longer treats backup as something to store, but as something to actively protect.

Security begins at backup.

Connect with us.

Investors Contact

Alexander Haunhorst

Managing Director

+49 152 542 531 26

alexander.haunhorst@valutistech.com

Valutis Technologies GmbH

Industriestr. 29

82194 Gröbenzell

www.valutistech.com