Security begins at backup.
We deliver immunity by design.

Investor Whitepaper

Valutis TECHNOLOGIES

GARDIEL

Pure Protection. Zero Compromise.

Executive Summary

Mit Gardiel entwickelt Valutis Technologies eine Sicherheitsarchitektur für eine Zeit, in der klassische Backup-Konzepte nicht mehr ausreichen. Wenn Ransomware heute nicht nur produktive Systeme, sondern gezielt auch Backup-Strukturen angreift, entscheidet sich genau dort, ob ein Unternehmen handlungsfähig bleibt oder in einen teuren Stillstand gerät.

Die Folgen solcher Angriffe reichen längst weit über IT-Ausfälle hinaus. Sie treffen Verfügbarkeit, operative Abläufe, Lieferfähigkeit, Vertrauen, Auditierbarkeit und im Extremfall die wirtschaftliche Stabilität eines Unternehmens. Recovery wird damit zur geschäftskritischen Fähigkeit.

Gardiel schließt diese Lücke. Das System schützt Daten bereits beim Schreiben, hält sie für die Wiederherstellung vollständig verfügbar und schafft die Grundlage für kontrollierte, verifizierbare Recovery. Statt Backup nur als passive Sicherung zu behandeln, macht Gardiel den Backup-Bestand zu einer aktiven Schutzebene der Cyber-Resilienz.

Für Unternehmen bedeutet das mehr Sicherheit, weniger operative Reibung und einen Wiederanlauf, der nicht auf Hoffnung, sondern auf Architektur basiert. Für Investoren ist Gardiel mehr als ein Cybersecurity-Produkt. Es ist der Ansatz für einen neuen Referenzstandard bei vertrauenswürdiger Datenresilienz.

Die Realität von Ransomware

Ransomware ist längst kein isoliertes IT-Risiko mehr. Sie zählt zu den stärksten Treibern von Cyber-Schäden und Cyber-Versicherungsverlusten und entwickelt sich in Frequenz, Professionalität und Schadenshöhe kontinuierlich weiter. Angriffe zielen heute nicht nur auf produktive Systeme, sondern bewusst auch auf Backups, weil genau dort über Wiederanlauf oder Stillstand entschieden wird.

Unabhängige Marktausblicke beziffern die jährlichen Opferschäden bis zum Beginn des nächsten Jahrzehnts auf über 245 Milliarden Euro. Für Unternehmen bedeutet das Produktionsunterbrechungen, Lieferausfälle, Reputationsschäden, regulatorischen Druck und wachsende Anforderungen von Versicherern und Auditoren.

Damit verschiebt sich die eigentliche Frage. Es geht nicht mehr nur darum, ob ein Angriff verhindert werden kann. Es geht darum, wie schnell und wie sauber ein Unternehmen nach einem Vorfall wieder arbeitsfähig wird. Recovery wird damit von einer operativen IT-Aufgabe zu einer Management-, Risiko- und Board-Level-Frage.

Die Lösung

Gardiel wird zwischen Corporate Network und Backup-Infrastruktur installiert und schafft dort eine neue Sicherheitslogik. Als hardwareverankertes Gateway mit unidirektionaler Datendiode schützt das System Daten bereits beim Schreiben und macht den Backup-Bestand zu einer aktiven Schutzebene.

Die Daten bleiben für die Wiederherstellung vollständig verfügbar, während eingeschleuste Schadsoftware in diesem Zustand nicht mehr ausführbar ist. Der Schutz entsteht damit nicht nachgelagert, sondern direkt am Write Path.

Ein zentraler Vorteil liegt darin, dass Gardiel bestehende Backup-Umgebungen nicht ersetzt, sondern ergänzt. Unternehmen können vorhandene Prozesse, Systeme und Investitionen weiter nutzen, während Gardiel genau die Schicht hinzufügt, auf die es im Ernstfall ankommt.

So funktioniert Gardiel

Die Funktionslogik von Gardiel folgt einer klaren Sequenz aus Backup, Forensik und Wiederherstellung.

Beim Backup gelangen Daten ausschließlich über die unidirektionale Datendiode in den geschützten Speicherbereich. Beim Schreiben werden sie in Echtzeit und mit einer für jede Gardiel-Instanz individuellen Obfuscation geschützt. Für die Wiederherstellung bleiben sie vollständig verfügbar, während Schadsoftware in diesem Zustand nicht mehr ausführbar ist.

Für Forensik und Bereinigung bleibt der gesamte Backup-Bestand auch im obfuskierten Zustand kontinuierlich überprüfbar. Ein vollständig isoliertes Verwaltungsnetz ermöglicht Monitoring, Analyse und gezielte Bereinigung. Der Zugang ist zusätzlich über einen Hardware Key abgesichert. Signaturen, YARA-Regeln und andere Bedrohungsindikatoren lassen sich jederzeit auf den Bestand anwenden, auch auf ältere Snapshots. So können Schadbestandteile gezielt erkannt, geprüft und entfernt werden, ohne dass eingeschleuste Software dabei aktiv wird.

Wenn Daten aus dem Backup wieder benötigt werden, wird der Datenpfad kontrolliert und über einen separaten physischen Hardware Key in den Recovery-Modus umgeschaltet. Aktiv ist dann ausschließlich die Richtung zurück ins Corporate Network. Während der Rückübertragung werden die Daten rücktransformiert und stehen sofort wieder in ihrer ursprünglichen, lesbaren Form zur Verfügung. Recovery wird so zu einem kontrollierten und reproduzierbaren Prozess.

Warum Gardiel anders ist

Gardiel verbindet mehrere Eigenschaften, die in dieser Kombination bislang einzigartig sind. Die unidirektionale Datendiode verhindert einen Rückkanal ins produktive Netzwerk. Die individuelle Obfuscation schützt Datenzustände bereits beim Schreiben. Der obfuskierte Bestand bleibt kontinuierlich prüfbar. Forensik und Bereinigung laufen in einem isolierten Verwaltungsnetz. Recovery erfolgt kontrolliert und in nur eine Richtung.

Aus dieser Kombination entsteht ein Sicherheitsniveau, das klassische Air-Gap-Logiken in ihrer Schutzwirkung aufgreift, ohne deren operative Nachteile zu übernehmen. Gardiel schafft Air-Gap-Sicherheit bei operativer Geschwindigkeit und ergänzt bestehende Backup-Landschaften, statt sie zu ersetzen.

Der Unterschied zu rein softwarebasierten Ansätzen liegt vor allem im Zeitpunkt und in der Art des Schutzes. Gardiel greift nicht erst dann ein, wenn ein Vorfall analysiert oder ein Restore vorbereitet wird. Der Schutz entsteht im Datenfluss selbst. Der Backup-Bestand bleibt verfügbar, prüfbar und für die Wiederherstellung vorbereitet.

Technologische Substanz und Proof Points

Die Basis von Gardiel besteht aus einem belastbaren technologischen Fundament. Dazu gehören mehr als 350 Patentansprüche in vier Patentfamilien sowie ein hardwareseitig validierter Funktionsnachweis. Damit ist Gardiel nicht nur geistiges Eigentum auf dem Papier, sondern technisch in Hardware nachvollziehbar und realisiert.

Diese Substanz wird ergänzt durch eine klare Produktlogik, einen investorenfähigen Kommunikationsstand und eine Architektur, die bereits heute marktseitig anschlussfähig ist. Für Auditoren, Versicherer, Partner und potenzielle Pilotkunden entsteht dadurch ein deutlich höheres Maß an Glaubwürdigkeit als bei rein theoretischen oder ausschließlich softwarebasierten Konzepten.

Für Investoren übersetzt sich das in Defensibility, Preispotenzial und bessere Voraussetzungen für Zertifizierung, Diligence und Markteintritt.

Kundennutzen

Unternehmen brauchen im Ernstfall mehr als gespeicherte Daten. Sie brauchen Zustände, die verfügbar, prüfbar und sauber wiederherstellbar sind. Genau darin liegt der Kundennutzen von Gardiel.

Die Architektur verhindert das Risiko, dass kompromittierte Backups zum Engpass der Wiederherstellung werden. Sie schafft einen dauerhaft überprüfbaren Bestand, reduziert die Abhängigkeit von manuellen Air-Gap-Prozessen und macht Recovery planbar. Das verkürzt Ausfallzeiten, senkt operative Komplexität und stärkt das Vertrauen in die eigene Wiederanlauffähigkeit.

Für regulierte und geschäftskritische Umgebungen ist das besonders relevant. Wo Verfügbarkeit, Integrität und Nachweisbarkeit gleichzeitig gefragt sind, bietet Gardiel eine technische Antwort auf genau diese Kombination.

Zielmarkt

Der erste Fokus liegt auf größeren mittelständischen Unternehmen mit verteilten IT- und OT-Strukturen, schlanken Security-Teams und einem hohen Bedarf an manipulationssicheren Backups sowie schneller Wiederherstellung. In diesen Umgebungen ist der Druck hoch, gleichzeitig sicher und operativ handlungsfähig zu bleiben.

Von dort aus eröffnet sich der Weg in regulierte und missionskritische Segmente wie Healthcare, Manufacturing, Public Sector und souveräne Cloud-Umgebungen. Gerade dort treffen hohe Anforderungen an Verfügbarkeit, Auditierbarkeit und Resilienz auf die Notwendigkeit, bestehende Systemlandschaften weiter zu nutzen.

Geschäftsmodell

Gardiel wird als Hardware-as-a-Service angeboten und schafft damit die Grundlage für planbare, wiederkehrende Umsätze. Das Modell verbindet Hardware, Wartung und Updates mit einer klaren Erweiterungslogik über zusätzliche Einheiten, forensische Services, Premium-SLAs und Training.

Aus Investorensicht ist dieses Modell attraktiv, weil es nicht auf Einmalerlöse setzt, sondern auf wiederkehrende Einnahmen, klare Paketierung und Ausbaupotenzial pro Standort oder Kundengröße. In einem Markt mit hoher Relevanz und hohem Leidensdruck entsteht daraus eine robuste kommerzielle Logik.

Patentstrategie

Das Patentportfolio schützt die Kernmethodik, während die Architektur bewusst auf standardnaher Hardware mit proprietärem Verfahren aufsetzt. Dadurch entsteht eine Kombination aus breitem Schutzraum und praktikabler Umsetzbarkeit.

Die bestehende Portfoliostruktur eröffnet zusätzlich Flexibilität über Teilanmeldungen und spätere strategische Erweiterungen. Für Investoren ist diese Strategie wichtig, weil sie technische Differenzierung, Verteidigbarkeit und Skalierung zugleich stärkt.

Nächste Entwicklungsschritte

Die nächsten Schritte konzentrieren sich auf die Finalisierung der Hardware, den Start der Zertifizierung, erste Pilotprojekte und den strukturierten Markteintritt in Deutschland. Perspektivisch kommen Themen wie Cluster Failover, Auto Restore, formale Zertifizierungen und vertikale Expansion in regulierte Branchen hinzu.

Langfristig entwickelt sich die Vision von Gardiel in Richtung eines gemanagten Resilienz-Netzwerks mit Telemetrie, intelligenter Anomalie-Erkennung und stärkerer Anschlussfähigkeit an Versicherer, Auditoren und Governance-Prozesse.

Funding Ask

Valutis akquiriert aktuell 1,5 Millionen Euro für eine Runway von 18 Monaten. Die Mittel dienen dazu, die Hardware zu finalisieren, die Zertifizierung zu starten, zehn bis fünfzehn Pilotprojekte umzusetzen und den Marktstart in Deutschland vorzubereiten.

Nach bisherigem Stand verteilen sich die Mittel auf Forschung und Entwicklung, Hardware und Staffing, Patentinternationalisierung, Zertifizierung und forensische Tooling-Anteile sowie Marketing und Sales. Zusätzlich sind gezielte Einführungen in Richtung Banken, Versicherer und kritische Infrastrukturpartner von hoher strategischer Relevanz.

Team

Hinter Valutis steht ein Team, das technologische Entwicklung, Cybersicherheit, Intellectual Property und unternehmerische Umsetzung zusammenbringt. Diese Kombination ist entscheidend, weil Gardiel nicht nur als Idee überzeugen muss, sondern als reales Produkt, als belastbare Schutzarchitektur und als investierbares Marktangebot.

Ergänzt wird das Team durch Kompetenzen in Produktdesign, Markenentwicklung und Marketing, damit Technologie, Produktwirkung und Go-to-Market in der nächsten Phase sauber zusammenlaufen können. Zusammen mit erfahrenen Stimmen aus technologie- und speicherbezogenen Umfeldern entsteht so ein Aufbau, in dem Produkt, Compliance, Marktauftritt und Skalierung eng aufeinander abgestimmt werden.

Investment Invitation

Valutis baut mit Gardiel an einem neuen Referenzstandard für vertrauenswürdige Datenresilienz. Wenn Recovery künftig beweisbar, schnell und hardwareverankert sein muss, dann ist jetzt der Zeitpunkt, diese Kategorie mitzugestalten.

Ein Investment in Gardiel beschleunigt Zertifizierung, Pilotprojekte und Markteintritt. Vor allem aber unterstützt es den Aufbau einer Sicherheitsarchitektur, die Backup nicht länger nur sichert, sondern aktiv schützt.

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