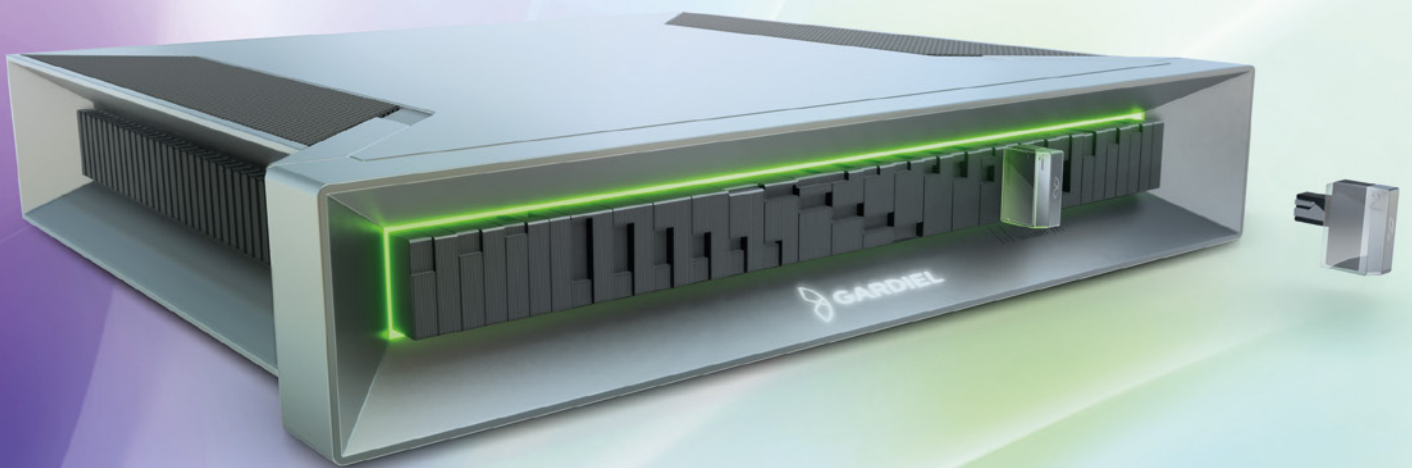


ENGLISH

Security begins at backup.

We deliver immunity by design.



 **GARDIEL**
**Pure
Protection.
Zero
Compromise.**



Protection, recovery, verifiability. In one architecture.

Gardiel turns your backup into an active part of modern cyber defense. A hardware-anchored gateway with a unidirectional data diode protects the storage environment, transforms data in real time, and enables controlled recovery without creating an additional attack path.

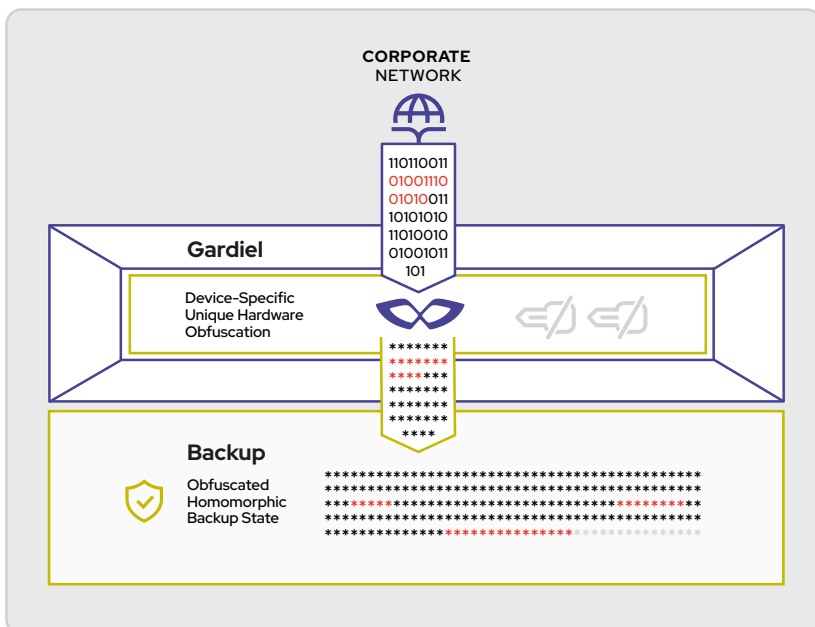
1

One way in Individual obfuscation Safe at write

The Gardiel gateway operates as a unidirectional data diode between the corporate network and the storage infrastructure. Data moves exclusively from the production network into the protected storage environment. There is no return path that an attacker could use to reach back into the corporate network.

At write time, data is obfuscated and transformed in real time at the hardware level, while remaining fully available for recovery. Malware or ransomware introduced into the system can no longer execute in that state.

A key part of Gardiel's protection lies in the individual configuration of each gateway. Every instance uses its own individual obfuscation, making it far more difficult to transfer attack patterns across installations. The result is an integrity-protected backup state as a reliable foundation for trustworthy recovery.



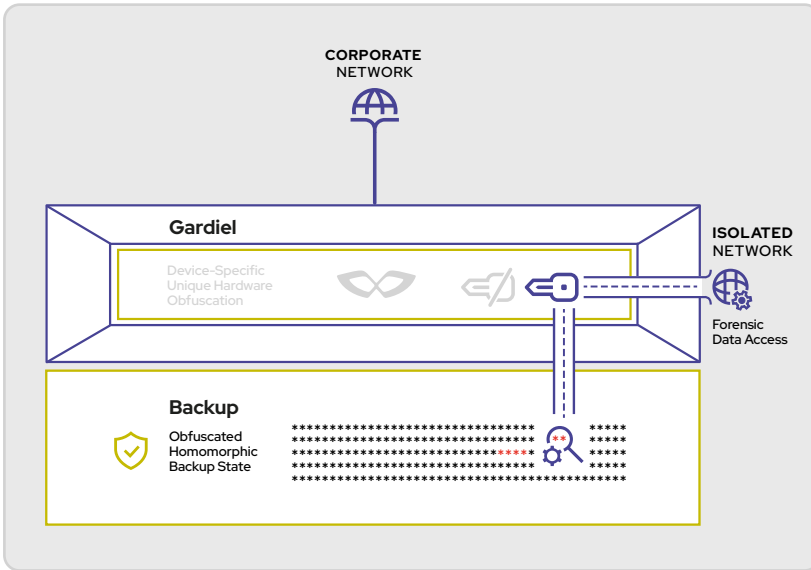
2

Continuously verifiable Threats safely detectable Always clean backup

The entire backup environment remains continuously inspectable, even in its obfuscated state, without allowing embedded malware to become active. Signatures, YARA rules, and other threat indicators can be applied at any time across the homomorphically obfuscated backup environment, including older snapshots.

Identified malicious components can be removed in a targeted manner, without sandbox processes and without the risk of propagation during analysis.

A fully isolated administrative network is available for monitoring, forensics, and remediation. Access is secured by a hardware key. This keeps the backup environment in a verifiably clean state and ready for controlled recovery at any time.

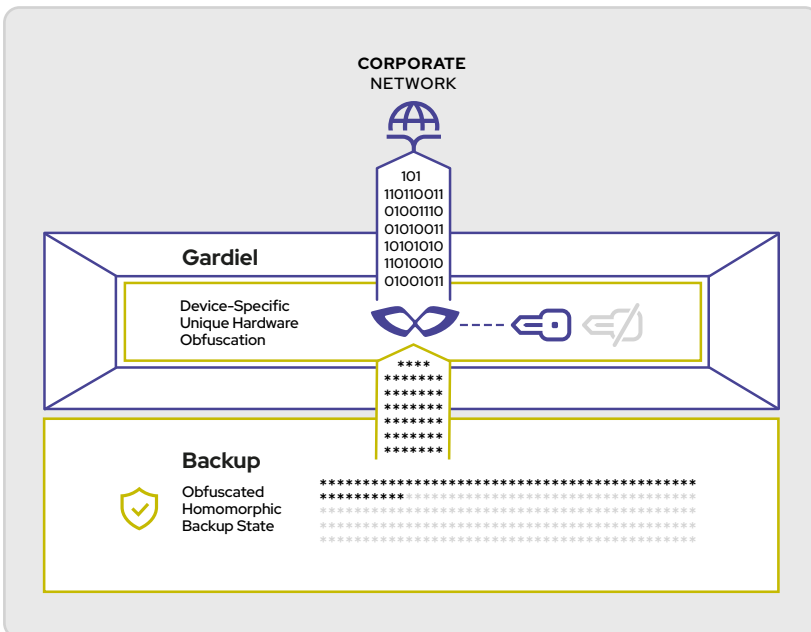
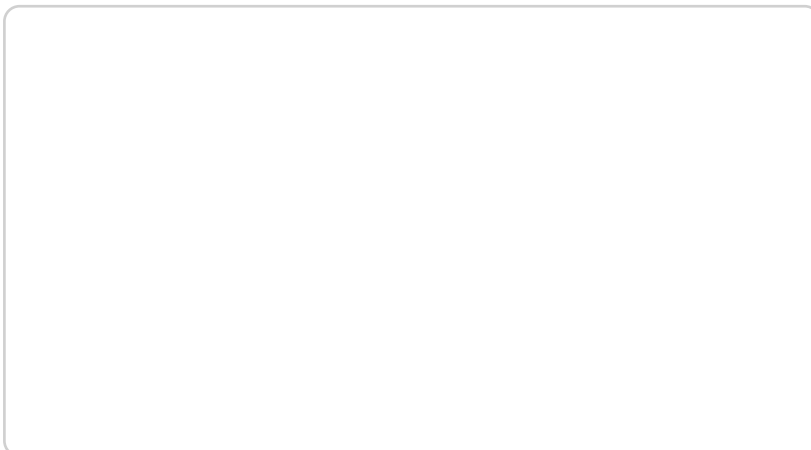


3

Controlled recovery One direction only Cleanly restored

When data is needed again, Gardiel's unidirectional protection logic remains intact. The data path is switched into recovery mode in a controlled manner using a physical hardware key. At that point, only the direction back into the corporate network is active. Parallel access in both directions is structurally impossible, so recovery does not create an additional attack path.

During the transfer back, the data is transformed back using the individual obfuscation and is immediately available again in its original, readable form. Recovery becomes a planned and repeatable process, without manual air-gap procedures, media breaks, or operational detours.



Trust is not built in a crisis. It is built before.

Valutis Technologies develops systems that bring backup security and trustworthy recovery together in a new way: with a hardware-based diode architecture, individual obfuscation, and a continuously verifiable backup environment.



Valutis Technologies GmbH

Industriestraße 29

82194 Gröbenzell, Germany

Phone +49 8142 4653 98-0

hello@valutistech.com

www.valutistech.com