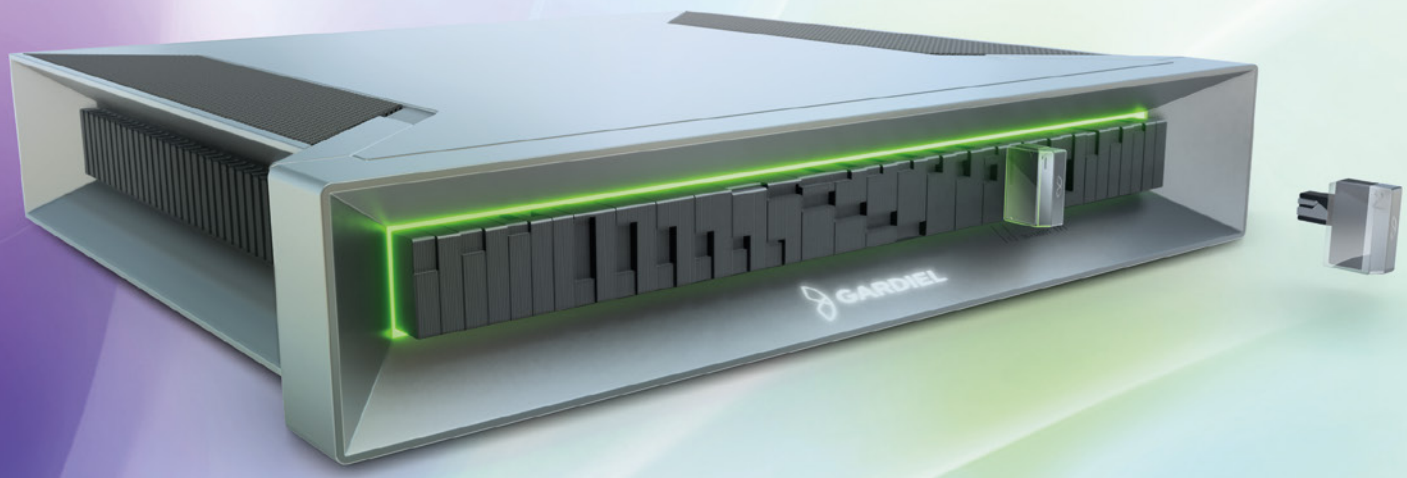
DEUTSCH

Security begins at backup.

We deliver immunity by design.



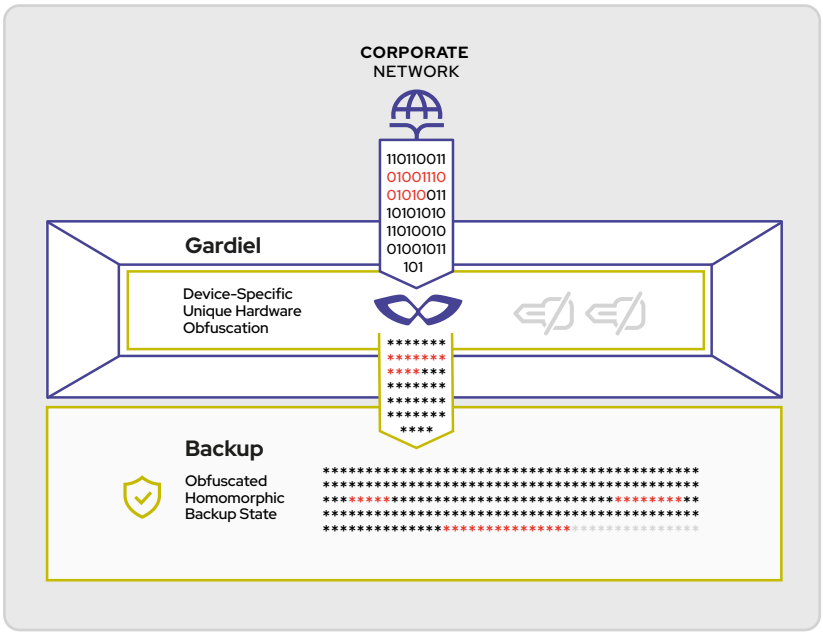
GARDIEL

Pure Protection. Zero Compromise.

GARDIEL

Schutz, Recovery, Prüfbarkeit. In einer Architektur.

Gardiel macht ihr Backup zu einem aktiven Teil moderner Cyberabwehr. Ein hardwareverankertes Gateway mit unidirektionaler Datendiode schützt den Speicherbereich, transformiert Daten in Echtzeit und ermöglicht eine kontrollierte Recovery, ohne einen zusätzlichen Angriffsweg zu schaffen.



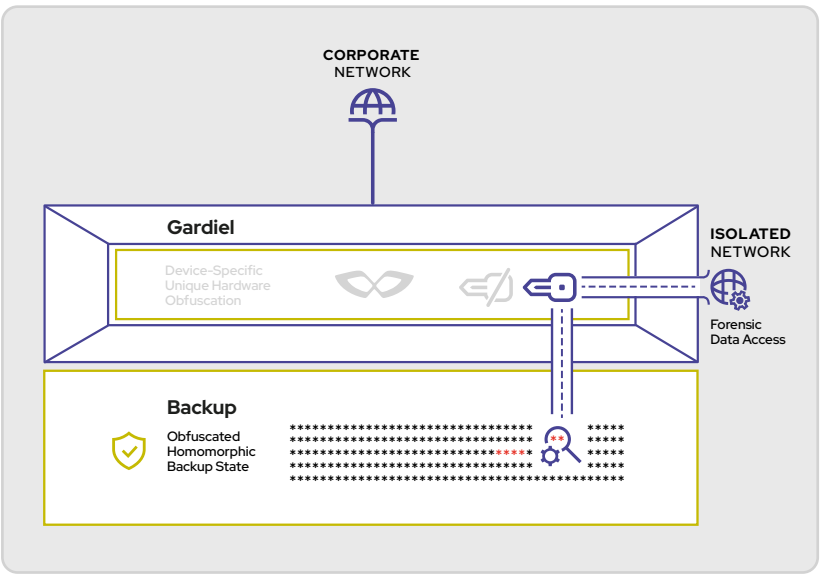
1

Datendiode »one way in« Individuelle Obfuscation Sicherheit beim Schreiben

Das Gardiel-Gateway wird als unidirektionale Datendiode zwischen Corporate Network und Speicherinfrastruktur betrieben. Daten fließen ausschließlich vom produktiven Netzwerk in den geschützten Speicherbereich. Ein Rückkanal, über den ein Angreifer zurück ins Corporate Network wirken könnte, existiert nicht.

Beim Schreiben werden die Daten auf Hardware-Ebene in Echtzeit obfuskiert und so transformiert, dass sie für die Wiederherstellung vollständig verfügbar bleiben. Eingeschleuste Schadsoftware oder Ransomware kann in dieser Form nicht mehr ausgeführt werden.

Der besondere Schutz entsteht durch die individuelle Konfiguration jedes Gardiel-Gateways. Jede Instanz verwendet ihre individuelle Obfuscation, sodass sich Angriffsansätze nicht auf andere Installationen übertragen lassen. Das schafft einen integritätsgesicherten Backup-Zustand als belastbare Grundlage für verlässliche Wiederherstellung.



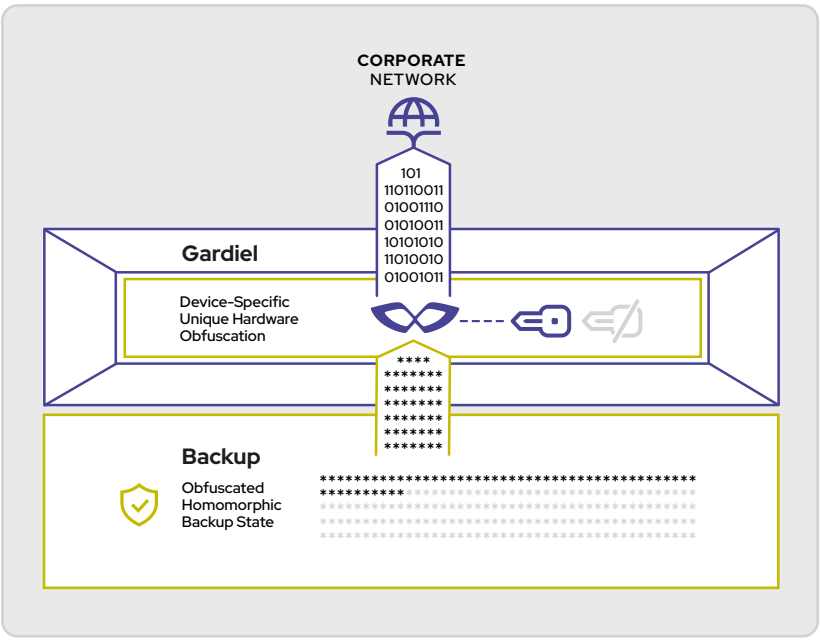
2

Kontinuierlich prüfbar Bedrohungen erkennbar Immer ein sauberes Backup

Der gesamte Backup-Bestand kann auch in seinem obfuskierten Zustand kontinuierlich überprüft werden, ohne dass eingeschleuste Schadsoftware dabei aktiv wird. Signaturen, YARA-Regeln und andere Bedrohungsindikatoren lassen sich jederzeit auf den homomorph obfuskierten Bestand anwenden, auch rückwirkend auf ältere Snapshots.

Identifizierte Schadbestandteile können gezielt entfernt werden, ohne Sandbox-Prozesse und ohne Risiko einer Ausbreitung während der Analyse.

Für Monitoring, Forensik und Bereinigung steht ein vollständig isoliertes Verwaltungsnetz zur Verfügung. Der Zugang ist über einen Hardware Key abgesichert. So bleibt der Backup-Bestand dauerhaft in einem verifiziert sauberen Zustand und jederzeit bereit für eine kontrollierte Wiederherstellung.



3

Kontrollierte Recovery Datendiode »one way out« Sauber wiederhergestellt

Wenn Daten wieder benötigt werden, bleibt die unidirektionale Schutzlogik des Gardiel-Gateways erhalten. Der Datenpfad wird über einen physischen Hardware Key kontrolliert in den Recovery-Modus umgeschaltet. Aktiv ist dann ausschließlich die Richtung zurück ins Corporate Network. Ein paralleler Zugriff auf Hin- und Rückweg ist konstruktionsbedingt ausgeschlossen. So entsteht auch im Wiederherstellungsfall kein zusätzlicher Angriffsweg.

Während der Rückübertragung werden die Daten mit der individuellen Obfuscation rücktransformiert und stehen unmittelbar wieder in ihrer ursprünglichen, lesbaren Form zur Verfügung. Recovery wird damit zu einem planbaren und reproduzierbaren Prozess, ohne manuelle Air-Gap-Abläufe, ohne Medienbrüche und ohne operative Umwege.

Vertrauen entsteht nicht im Ernstfall. Sondern davor.

Valutis Technologies entwickelt Systeme, die Backup-Sicherheit und vertrauenswürdige Recovery neu zusammenführen: mit hardwarebasierter Diodenarchitektur, individueller Obfuscation und kontinuierlich prüfbarem Backup-Bestand.

Valutis
TECHNOLOGIES

Valutis Technologies GmbH
Industriestraße 29
82194 Gröbenzell
Tel. +49 8142 4653 98-0
hello@valutistech.com
www.valutistech.com