OMNARETH

SOLUTION BRIEF

Payments Fraud Prevention

Pay the vendor, not the impostor: stop bank-detail fraud and payment diversion before money moves

The challenge

Every business pays suppliers, and fraudsters know it. An email from a lookalike domain asks to change a vendor's bank details; a clerk updates the record; the next invoice is paid to an account the fraudster controls. The same account then turns up on other vendors. Each step looks routine to the person doing it, and afterwards nobody can prove who knew what, when.

The solution

Omnareth checks every vendor bank change and every payment request against the vendor master before money moves. It answers allow, flag or deny with the reasons, holds the fraudster's account responsible (never the vendor, never the clerk), recognizes that account when it is pushed onto another vendor, and seals every decision so it can be proven later.

11	75 ms	9/9
reference rules for vendor payments	median fraud-checked, audited decision, lab test	reference scenario decisions correct and verified on chain

How it fits

Your ERP or payment platform sends each bank-detail change and payment request to Omnareth and releases only what it allows. The vendor master records each vendor's verified email domain, the bank accounts verified by callback, its usual invoice limit and the invoices already paid. Nothing else in the process changes.

> **Evidence for auditors and insurers**
>
> Every decision stores the vendor record, the request and the exact rules evaluated, with what was known about the account, under a SHA-256 integrity hash anchored on the Omnareth chain.
>
> Edits to the record, including ones hidden by recomputing the stored hash, fail verification.

Next step: run the scenario with your team (one command, every record verified), then scope a shadow-mode pilot on your payment run. See the Pilot Program Guide.

© 2026 Habify Labs, Inc. All Rights Reserved. · Omnareth

What it stops

THREAT	HOW OMNARETH CATCHES IT	DECISION
Bank detail change fraud	New bank account not verified by callback to a known contact	DENY
Business email compromise	Change request from a domain other than the vendor's verified domain	DENY
Payment diversion	Payment to an account that is not a verified account of the vendor	DENY
Duplicate invoice	Invoice number already paid	DENY
Self-approval	Requester and approver are the same person	DENY
Paying a vendor on hold	Vendor is on hold or blocked	DENY
Unusual amount	Invoice above the vendor's limit	FLAG
Known fraud account	A bank account, domain or person blocked on the watchlist	DENY
Watched identity	An identity under watch, added by an analyst or automatically	FLAG
Repeat offender	An identity implicated in 2 or more denied events in the last 30 days	FLAG
One account, many vendors	An account or domain implicated in denials on 2 or more other vendors in 24 hours	FLAG

The reference campaign: business email compromise against 3 vendors

#	EVENT	DECISION	FRAUD CASES
1	Genuine Northwind Steel invoice to its verified account	ALLOW	
2	'Northwind' emails new bank details from northwlnd-steel.com	DENY	
3	A clerk keys the new account and requests payment	DENY	Repeat offender opened for the account; account watched
4	Same account sent to Fabrikam Logistics from another lookalike	DENY	
5	Same account on a Tailspin Packaging payment	DENY	One account across three vendors: case opened
6	Fabrikam invoice submitted a second time	DENY	
7	A clerk approves their own payment	DENY	
–	Analyst confirms the case	-	Account blocked for every vendor
–	An insider adds the account to Tailspin's verified accounts	-	
8	Payment to the now "verified" account	DENY	
9	Genuine Tailspin invoice	ALLOW	

© 2026 Habify Labs, Inc. All Rights Reserved. · Omnareth