OMNARETH

SOLUTION BRIEF

Cybersecurity Fraud Prevention

Let the owner in. Not the attacker.

The challenge

Attackers test stolen passwords across thousands of accounts. Each attempt looks like one user mistyping; the campaign only shows across accounts.

The solution

Account takeover runs on stolen credentials: credential stuffing, MFA push bombing, recovery emails changed from unknown devices, and help desks talked into bypassing MFA. Omnareth checks every sign-in, security change and privileged action before it is granted, and recognizes the attacker's address or device across accounts.

14
reference rules for cybersecurity

75 ms
median fraud-checked, audited decision, lab test

8/8
reference scenario decisions correct and verified on chain

How it fits

ELEMENT	IN THIS SOLUTION	WHAT IT COVERS
The record	The account	Status, the devices the account has verified, the roles it holds and how much data it may export.
The events	Sign-ins, changes, actions	A sign-in needs the password and MFA; a security change from a new device needs step-up; an action needs a granted role, within limits.
The memory	One address, many accounts	The attacker's address, device and recovery email are held responsible, never the account owners.

> **Evidence for auditors and regulators**
>
> Every decision stores the record, the request and the exact rules evaluated, with what was known about everyone involved, under a SHA-256 integrity hash anchored on the Omnareth chain. Edits, even covered-up ones, fail verification.

Next step: run the scenario with your team (`examples/cybersecurity-fraud/demo.sh`, one command, every record verified), then scope a 90-day shadow-mode pilot. See the Pilot Program Guide.

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

What it stops

RULE	WHAT OMNARETH CHECKS	DECISION
Account Not Active	Locked or disabled accounts cannot sign in or act.	DENY
Export Over Limit	A data export may not exceed the account's export limit.	DENY
Role Not Granted	A privileged action needs a role granted to the account.	DENY
Security Change Unverified	Password, MFA or recovery-email changes from a new device need step-up.	DENY
Wrong Password	A sign-in needs the correct password.	DENY
Impossible Travel	Deny a sign-in that would require travelling faster than an airliner since the last one.	DENY
MFA Fatigue	Three or more declined push prompts in one sign-in indicate push bombing.	DENY
MFA Not Passed	A sign-in needs a completed second factor.	DENY
New Device	Flag a successful sign-in from a device the account has not verified.	FLAG
Source Across Accounts	Flag an IP, device or recovery email implicated in denials on 2+ other accounts in 24h.	FLAG
Session Token Reuse	A session token belongs to one account; seen on another, it was likely stolen.	FLAG
Repeat Offender	Flag events involving an identity implicated in two or more denied events in the last 30 days.	FLAG
Blocked Identity	Identities blocked on the fraud watchlist may not take part in any account event.	DENY
Watched Identity	Identities under watch may proceed only with a flag for review.	FLAG

The reference scenario

#	EVENT	DECISION	FRAUD CASES
1	Genuine sign-in from a known laptop	ALLOW	
2	Credential stuffing: wrong password from the attacker's address	DENY	
3	MFA push bombing with a leaked password, same address	DENY	Repeat offenders; address and device watched
4	Recovery email changed from an unknown device	DENY	One address across three accounts: case opened
5	Genuine sign-in from the owner's new phone	FLAG	
6	An employee exports 48,000 records against a 5,000 limit	DENY	
–	Analyst confirms the address case	-	Address blocked everywhere
7	After the helpdesk trusts its device, the attacker signs in with MFA bypassed	DENY	
8	Genuine sign-in	ALLOW	

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