

Mimoto Continuous Verification

Continuous person-based verification for the modern cyber world.



OVERVIEW

Traditional cybersecurity relies on credentials, tokens, and anomaly detection, but adversaries have evolved faster than the systems protecting organizations.

Compromised credentials, deepfakes, and “agentic AI” actors now routinely get past PAM and identity management tools. Meanwhile, the spread of AI in cyberattacks is driving exponential growth in the number of attacks and their sophistication. Mimoto introduces a new cybersecurity paradigm: **person-based continuous verification**. Instead of securing accounts, Mimoto secures people, continuously verifying the real human behind every credential, account, or access point, in real time.

THE PROBLEM: CREDENTIALS CAN NO LONGER BE TRUSTED

For cybersecurity managers, the work has shifted from defending the network perimeter to verifying the person, continuously. Yet current tools depend on credentials and static authentication events that attackers can easily hijack.

Credential compromise and account takeover

Adversaries exploit stolen or shared credentials across hybrid cloud and SaaS systems.

AI-driven impersonation

Deepfakes and autonomous agents can now mimic human logins, voice, or behavioral patterns with alarming precision.

Insider threats and privileged abuse

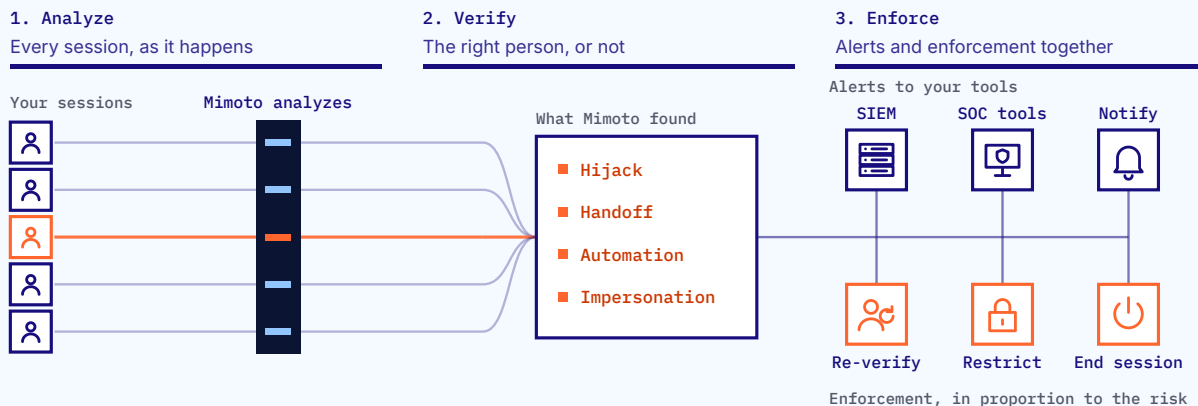
Even authorized users may act maliciously or from unsanctioned regions, violating regulatory or security policy.

Regulatory gaps

NIST, OMB, and Zero Trust frameworks introduce significant user friction while demanding continuous verification of user identity and behavior, something legacy IAM cannot provide.

The result: cyber leaders face blind spots inside their most trusted systems, where attacks unfold quietly, often by valid users doing invalid things.

ANALYZE, VERIFY, ENFORCE



Sessions pass through Mimoto. It finds the ones where the person does not match and responds in real time, with alerts and enforcement together, in proportion to the risk. Illustration only.

THE SOLUTION

Person-based, all session long

Mimoto's patent-pending technology uses multidimensional behavioral "fingerprints," a fusion of AI-driven advanced pattern matching and anomaly detection, to recognize and respond to identity misuse the instant it occurs.

Instead of relying on static credentials or behavioral baselines, Mimoto builds a live, multidimensional behavioral profile of each individual and continuously verifies that the person behind every session is genuine, authorized, and acting within their sanctioned context.

WHY IT MATTERS TO CYBER LEADERS

Mimoto aligns with the Zero Trust mandates for "continuous identity evaluation." Its person-based architecture delivers what existing IAM and PAM systems cannot: the ability to see and stop human or agentic activity that looks legitimate but behaves maliciously.

- **Real-time, autonomous defense.** Machine-speed response prevents lateral movement and data theft.
- **Credential-independent.** Operates even if credentials or tokens are compromised.
- **Mission adaptability.** Deployable in tactical networks, cloud workloads, and hybrid IT.
- **Privacy-preserving design.** No PII is collected or stored, and users are never followed.

Core capabilities

Person-specific recognition

Detects when a credential or generic account is used by anyone other than the verified individual, even when authentication is bypassed.

Real-time response

Instantly interrupts ransomware activity, data theft, or policy violations.

Behavioral context awareness

Recognizes location, device, access pattern, and mission context to confirm legitimacy.

Agentic AI detection

Identifies and blocks bots or synthetic identities posing as human users.

Cloud-agnostic deployment

Operates at any access point: managed endpoint, SaaS, shared workstation, or BYOD, even in air-gapped or limited-connectivity environments.

Popular use cases

01 Offshore and remote developers

Verify that only contracted personnel, in an authorized location, access code repositories or mission systems, not unauthorized offshore actors or AI proxies.

02 Privileged user oversight

"Watching the watchers": detect and stop unauthorized activity from admin or IT staff with elevated privileges.

03 Data loss prevention

Identify who is accessing sensitive datasets, and act automatically if access context violates policy.

04 Ransomware prevention

Block malicious behavior at the human level before encryption or exfiltration begins.

05 Regulated or classified environments

Add person-level continuous verification to meet compliance for financial, healthcare, or national security operations.

06 Supply chain and open-source protection

Detect and respond to backdoor access injected into the software supply chain or open source.

From "Who has access?" to "Who is actually behind the screen?" As cybercriminals weaponize AI and get in through trusted accounts, cybersecurity must verify users continuously, not at login, but throughout every interaction.

ABOUT MIMOTO

Is this a real human? Is it the right human?

Mimoto provides person-based continuous verification. It recognizes and responds in real time when a user is impersonated by a person or an agent, a session is taken over, or a credential is shared or compromised.

See Mimoto catch the wrong person in a live session.

Schedule a Conversation with the Mimoto team at mimoto.ai/contact.

MIMOTO