CLOSING THE IDENTITY GAP

Why Legacy Security Solutions Cannot Answer the Most Critical Question in Security: Who Is Actually at the Keyboard?

A Mimoto White Paper | 2026

EXECUTIVE SUMMARY

Modern enterprises invest heavily in Identity and Access Management (IAM), Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), and anomaly detection platforms. These tools collectively manage credentials, aggregate logs, correlate events, and flag statistical outliers. Yet despite billions in annual spending, identity-based attacks continue to dominate the threat landscape. Credential abuse accounted for 22% of all data breaches in 2025, 60% of breaches still involved the human element, and AI-enhanced attacks, from deepfake impersonation to industrial-scale brute force, are accelerating the crisis.

The reason is deceptively simple: none of these technologies verify the person behind the session. They authenticate credentials, not people. Once a valid username and password or session token is presented, every downstream system trusts the session implicitly, regardless of who is actually operating it. Mimoto's Person-Based Identity Engine closes this gap by continuously verifying the real-world individual interacting with a system in real time, shifting the security paradigm from credential trust to person trust.

THE PROBLEM: A CREDENTIAL IS NOT A PERSON

The entire digital security stack is built on a foundational assumption: that the entity presenting a credential is the person to whom that credential was issued. This assumption has always been fragile; in 2025, it became untenable. Credential theft surged 160% year over year, with 1.8 billion login credentials stolen in the first half of the year alone. Session hijacking through stolen cookies now enables attackers to bypass even MFA and passkeys entirely, with 17.3 billion stolen session cookies circulating on the dark web in 2024.

When an attacker authenticates with valid stolen credentials, they inherit the legitimate user's identity in the eyes of every security tool in the stack. IAM grants access. Zero Trust architectures validate the session. SIEM logs the activity as normal. UEBA baselines absorb the behavior. The attacker operates inside a cocoon of assumed trust, often for weeks or months before detection. The average breach involving stolen credentials takes 292 days to identify and contain, the longest of any attack vector.

Where Each Layer Falls Short

IAM and SSO systems are gatekeepers, not guardians. They verify that a credential is valid at the moment of authentication, then step aside. They have no mechanism to confirm that the same person remains at the keyboard five minutes, five hours, or five days later. Session tokens persist. Credentials can be shared, stolen, or replayed. IAM answers the question "is this credential valid?" but never "is this the right person?"

© 2026 Mimoto, Inc.

SIEM platforms aggregate and correlate log data across the enterprise. They excel at identifying known attack patterns through rules and signatures, but they operate on metadata: source IPs, timestamps, event codes. They can tell you that an account accessed a resource at 2:47 AM. They cannot tell you whether it was the account holder, a colleague borrowing the account, or an adversary operating from halfway around the world.

UEBA and anomaly detection systems represent the most advanced attempt to address this gap, but they approach the problem from the wrong direction. They build behavioral baselines and flag statistical deviations: unusual login times, atypical data access volumes, abnormal geographic patterns. The critical weakness is that anomaly detection generates alerts on deviations, not on identities. A skilled attacker who mimics the legitimate user's behavior patterns, or a compromised insider acting within their normal role, generates no anomaly. Meanwhile, legitimate users who change projects, travel, or adopt new tools flood security teams with false positives.

THE ACCELERANT: AI-ENHANCED ATTACKS AND INDUSTRIAL-SCALE CREDENTIAL ASSAULT

The identity gap described above was already a critical vulnerability. Artificial intelligence has transformed it into an existential one. AI is not introducing fundamentally new attack categories; it is supercharging existing identity-based techniques, making them faster, more convincing, and vastly more scalable. The result is a threat environment where credential-based attacks are now automated, personalized, and increasingly indistinguishable from legitimate activity.

AI-Powered Social Engineering and Deepfake Fraud

AI-generated deepfakes have moved from a theoretical concern to a proven attack vector. A Gartner survey found that 62% of organizations reported experiencing a deepfake attack in the past twelve months. By early 2025, AI-supported phishing represented more than 80% of observed social engineering activity worldwide, according to ENISA's 2025 Threat Landscape report. The FBI's 2025 IC3 report logged a 37% rise in AI-assisted business email compromise, and deepfake incidents in the first quarter of 2025 alone exceeded the total for all of 2024.

The consequences are not abstract. In one widely reported incident, attackers used AI-generated deepfake video and voice cloning to impersonate a company's CFO and several colleagues on a live video call, convincing an employee to execute 15 wire transfers totaling $25.6 million. The attackers never breached a firewall or exploited a software vulnerability. They bypassed the most critical security control of all: the human judgment that determines whether the person on the other end is who they claim to be. This is precisely the kind of identity verification gap that IAM, SIEM, and UEBA are structurally unable to address.

AI has also collapsed the barrier to entry for sophisticated social engineering. Attackers now use large language models to generate highly personalized, grammatically flawless phishing messages at scale, eliminating the spelling errors and awkward phrasing that once served as reliable warning signs. Approximately one-third of phishing emails analyzed in early 2025 contained patterns consistent with LLM-generated text. Voice cloning technology requires as little as three seconds of source audio to produce an 85% voice match, with that audio easily scraped from social media, webinars, or corporate presentations. Deepfake-as-a-service platforms have made this technology accessible to cybercriminals at every skill level.

© 2026 Mimoto, Inc.

Brute Force at Unprecedented Scale

While AI enhances the sophistication of social engineering, it also amplifies the blunt-force end of the attack spectrum. In early 2025, the Shadowserver Foundation detected a massive brute force campaign targeting VPN devices from Palo Alto Networks, Ivanti, and SonicWall, leveraging nearly 2.8 million IP addresses daily to attempt credential guessing at industrial scale. The campaign, which used compromised MikroTik, Huawei, Cisco, and ZTE routers as attack infrastructure, originated primarily from Brazil, Turkey, Russia, Argentina, and Morocco. The attacks targeted firewalls, VPN gateways, and other internet-facing security devices, precisely the infrastructure organizations rely on to protect their perimeters.

This campaign was not an isolated event. Throughout 2025, Palo Alto Networks' GlobalProtect VPN portals faced repeated waves of credential-based attacks of escalating intensity. In April, GreyNoise observed 24,000 unique IP addresses scanning GlobalProtect login portals. By November, a fresh surge produced 2.3 million malicious scan sessions, with activity intensifying 40-fold within a single 24-hour period. In December, the attacks escalated further: over 1.7 million login sessions targeted GlobalProtect portals in just 16 hours, followed by an immediate pivot to Cisco SSL VPN endpoints. The attacks originated from more than 10,000 unique IP addresses hosted by a single German infrastructure provider, demonstrating the hallmarks of centralized, professional-grade automation.

These campaigns underscore a fundamental reality: brute force attacks at this scale are fully automated and operate continuously. They do not require human operators to sit at keyboards guessing passwords. They run around the clock, probing millions of endpoints, and they only need to succeed once. When they do, the resulting valid credential is indistinguishable from a legitimate login. IAM authenticates it. SIEM logs it as normal. UEBA has no baseline deviation to flag. The attacker is inside the network, and no existing tool in the traditional security stack knows it.

Why AI Makes the Identity Gap More Dangerous

AI amplifies the identity gap in three compounding ways. First, it increases the volume and velocity of credential attacks, as the brute force campaigns above demonstrate. Second, it improves the quality of social engineering, enabling attackers to impersonate legitimate users with voice clones, deepfake video, and AI-written communications that are nearly impossible to distinguish from genuine interactions. Third, and most critically, it enables attackers to blend in after gaining access, using AI to study and mimic legitimate user behavior patterns, making anomaly-based detection even less effective than it already was.

The traditional security stack's response to each of these threats is to recommend stronger authentication: better passwords, multi-factor authentication, passkeys. These are necessary measures, but they address only the front door. They do nothing once an attacker is inside with valid credentials, whether obtained through brute force, phishing, session hijacking, or deepfake-enabled social engineering. The question remains unanswered by every tool in the conventional stack: is the person using these credentials right now the person they were issued to?

THE PARADIGM SHIFT: CONTINUOUS PERSON-BASED VERIFICATION

Mimoto approaches identity security from a fundamentally different angle. Rather than monitoring what credentials are doing or flagging statistical anomalies in behavior, Mimoto continuously verifies who is

© 2026 Mimoto, Inc.

performing each action. The platform builds AI-generated identity profiles that are unique to each individual and uses real-time pattern matching to confirm the person behind every session, every interaction, and every access request.

This is not behavioral analytics dressed in new language. Traditional UEBA compares an entity's current actions against that entity's historical baseline and asks "is this behavior normal for this account?" Mimoto asks a fundamentally different question: "is this the same person who was verified when this profile was created?" The distinction is critical. A UEBA system cannot tell you that a contractor is using an executive's shared admin credentials. Mimoto can, because it is matching the person, not the credential.

How Mimoto Works: The Identity Detection and Response Stack

Mimoto's architecture is purpose-built to layer person-based verification across the entire enterprise without disrupting existing security investments. The following diagram illustrates how Mimoto integrates with and enhances each tier of the security stack, from identity and access at the top through detection, response, and automated enforcement at the bottom.

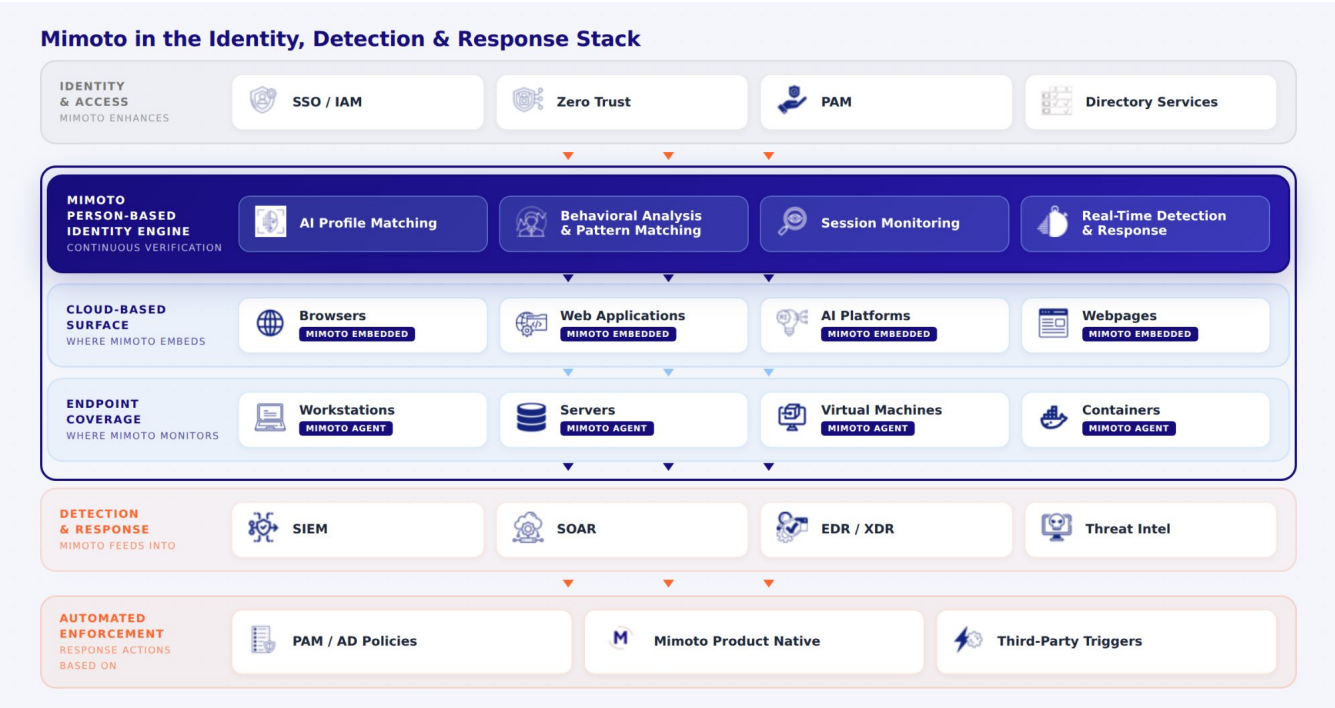

Figure 1: Mimoto in the Identity, Detection & Response Stack

At the top of the stack, Mimoto enhances existing IAM infrastructure including SSO, Zero Trust, PAM, and directory services. Rather than replacing these investments, Mimoto adds a person-verification layer that transforms credential-based trust into person-based trust. The Mimoto Person-Based Identity Engine sits at the core, performing four interconnected functions: AI Profile Matching builds and maintains unique identity profiles for each individual; Behavioral Analysis and Pattern Matching compares real-time interactions against verified person profiles rather than statistical baselines; Session Monitoring tracks identity continuity throughout active sessions; and Real-Time Detection and Response enables immediate action when a person-identity mismatch is detected.

© 2026 Mimoto, Inc.

Mimoto deploys across both cloud-based surfaces and endpoints. Mimoto Embedded integrates directly into browsers, web applications, AI platforms, and webpages, providing person verification at the application layer. Mimoto Agent deploys to workstations, servers, virtual machines, and containers to cover endpoint-level identity verification. This dual-surface approach ensures that a person's identity is verified regardless of how or where a user accesses enterprise resources.

The platform feeds verified identity intelligence into existing detection and response infrastructure including SIEM, SOAR, EDR/XDR, and threat intelligence platforms. This enrichment transforms the value of these tools: a SIEM alert that previously read "anomalous access detected" now reads "access by unverified individual on verified user's account." At the enforcement layer, Mimoto's identity signals drive automated response actions through PAM and AD policies, Mimoto's own native response capabilities, or taking action based on non-traditional third-party triggers.

THE GAP IN DETAIL: WHAT EXISTING TOOLS MISS

Credential Sharing and Insider Threats

Shared credentials, particularly for administrative and privileged accounts, are pervasive in enterprise environments. When multiple individuals use the same account, IAM sees a single authenticated entity. SIEM logs a single identity. UEBA builds a blended behavioral baseline that belongs to no one individual. Mimoto identifies exactly which person is using a shared account at any given moment, enabling accountability and attribution that existing tools simply cannot provide.

Session Hijacking and Token Theft

Modern attackers increasingly bypass authentication entirely by stealing active session tokens or cookies. Once in possession of a valid session, the attacker inherits full access without ever touching a password or MFA prompt. IAM never sees a new login. SIEM sees continued activity from an "authenticated" user. UEBA may see no anomaly if the attacker operates within normal parameters. Mimoto's continuous verification detects the identity shift the moment a session changes hands, regardless of whether the token is valid.

Credential Stuffing and Account Takeover

When attackers use stolen credentials from one breach to access accounts at another organization, the login appears entirely legitimate. The credentials are valid. The access patterns may be within normal bounds. There is nothing for anomaly detection to flag. Mimoto detects that the person presenting the credential does not match the verified profile associated with that account, triggering an alert or automated response before data is exfiltrated.

Sophisticated Adversaries Who Blend In

Nation-state actors and advanced persistent threats are trained to mimic legitimate user behavior. They access the same systems, at the same times, using the same protocols as the compromised user. UEBA baselines absorb this behavior as normal. Anomaly detection has nothing to detect. Mimoto's person-based approach is resilient against this because it is not looking for anomalies; it is verifying identity. An adversary can perfectly mimic a user's behavior, but they cannot become the person.

© 2026 Mimoto, Inc.

THE STRATEGIC CASE FOR CONTINUOUS PERSON VERIFICATION

The security industry has spent decades optimizing around credential trust. Stronger passwords. Multi-factor authentication. Zero Trust frameworks. Behavioral analytics. Each represents an incremental improvement to the same foundational model. Mimoto represents a fundamentally different approach: instead of making credentials harder to steal, it makes stolen credentials impossible to use undetected.

This shift has cascading benefits across the security organization. False-positive rates drop dramatically because person verification is a binary determination, not a statistical estimate. Mean time to detection collapses because identity mismatches are flagged in real time rather than discovered during forensic investigation months later. Compliance posture improves because organizations can demonstrate continuous verification of who accessed what, not just which credential was used. And existing security investments in IAM, SIEM, SOAR, and EDR become more valuable because they are now enriched with person-level identity intelligence.

Key Statistics Underscoring the Need

- **22%** of all data breaches in 2025 began with stolen credentials (Verizon DBIR)
- **292 days** average time to identify and contain a credential-based breach (IBM)
- **1.8 billion** login credentials stolen in the first half of 2025 (Flashpoint)
- **2.8 million** IP addresses used daily in a single brute force campaign against VPN devices (Shadowserver)
- **62%** of organizations experienced a deepfake attack in the past 12 months (Gartner)
- **80%+** of social engineering activity in early 2025 was AI-supported (ENISA)
- **60%** of breaches involved the human element (Verizon DBIR)
- **$4.81M** average cost of a breach involving stolen credentials (IBM)

CONCLUSION

The question at the center of every breach investigation is the same: who was it? Not which credential was compromised, not which system was accessed, but who was actually behind the keyboard. IAM, SIEM, UEBA, and anomaly detection platforms were never designed to answer this question. They manage credentials, aggregate logs, and flag statistical outliers, but they operate in a world where a valid credential is treated as a valid identity. AI-enhanced attacks, from deepfake impersonation to industrial-scale brute force, have made this assumption more dangerous than ever.

Mimoto's continuous person-based verification closes this gap by shifting the unit of trust from the credential to the individual. By continuously verifying the real-world person behind every session through AI profile matching, behavioral pattern analysis, and real-time detection and response, Mimoto addresses the root cause of identity-based attacks rather than their symptoms. In a threat landscape where attackers wield AI to steal credentials at scale, clone voices and faces, and operate undetected inside enterprise networks, knowing who is at the keyboard is not a luxury. It is a necessity.

To learn more about how Mimoto can close the identity gap in your organization, visit **mimoto.ai**

© 2026 Mimoto, Inc.