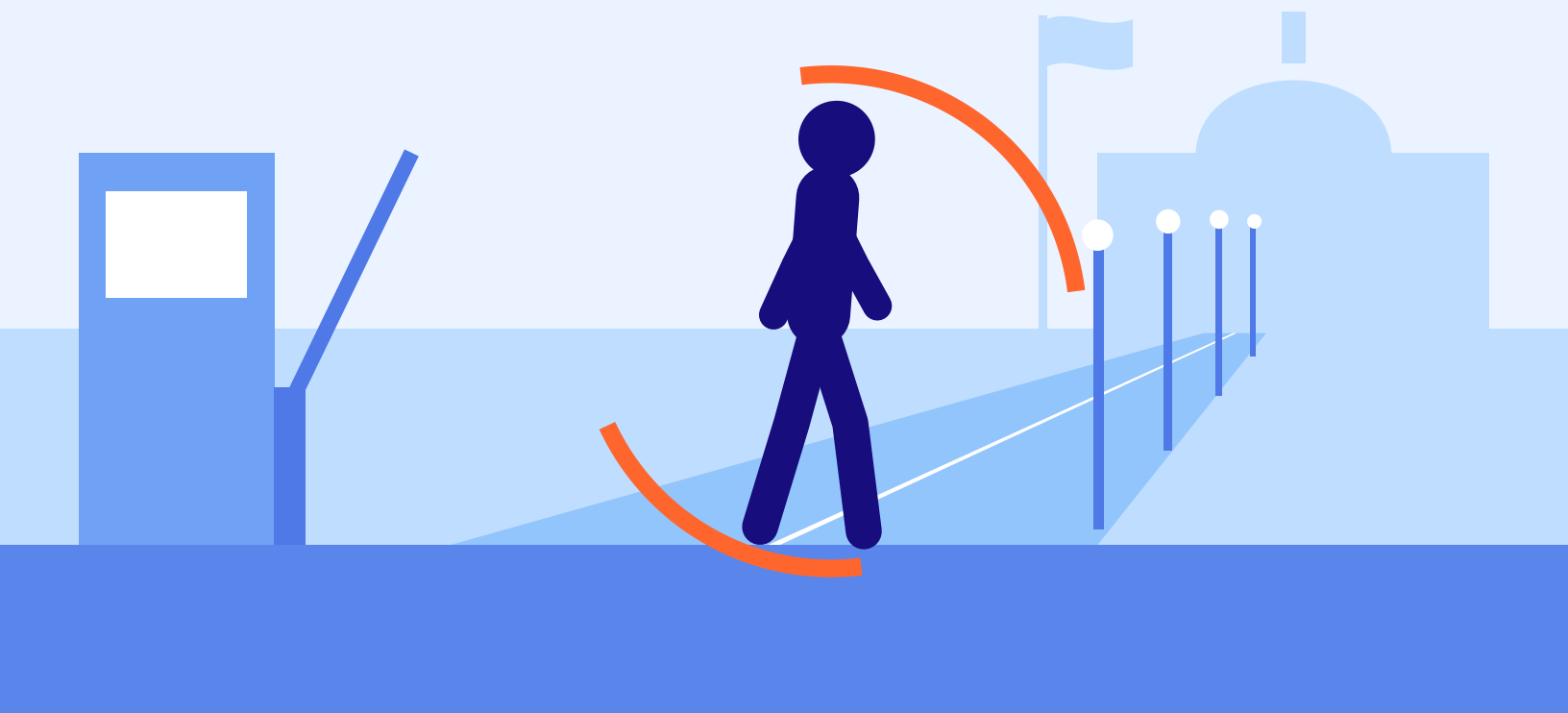




MIMOTO WHITE PAPER

Extending Zero Trust Through Continuous Identity Assurance

Persistent Human Identity Verification: Picking up Where Zero Trust Ends

September 2026

MIMOTO

At a glance

- Most Zero Trust architectures verify the person once, at login, then trust the token, ticket, or cookie that carries the session.
- NIST SP 800-207 and the CISA Zero Trust Maturity Model already call for identity to be evaluated continuously, not only when access is granted.
- Nation-state adversaries do not need to defeat the login. They need only to survive it, inside valid, authenticated sessions.
- Continuous Identity Assurance extends verification through the whole session and builds on the ICAM investments already in place.

Continuous Identity Assurance transforms identity from a static event into a dynamic security signal.

WHO SHOULD READ IT

Federal CISOs, Zero Trust program leads, and ICAM architects.

Published **September 2026**

Length **21 pages**

INSIDE

01	Executive Summary	3
02	The Identity Gap in Zero Trust	4
03	The Frameworks Already Call for It	7
04	Emerging Threats to Identity Assurance	8
05	Nation-State Adversaries: Why Point-in-Time Verification Fails	11
06	Continuous Identity Assurance	13
07	Agentic Zero Trust Attacks: Two Questions, One Architecture	14
08	Supporting the Pillars of Zero Trust	15
09	Alignment with Zero Trust Maturity Outcomes	17
10	Integration Within Existing ICAM Ecosystems	17
11	Enabling Partner, Subsidiary, and Supply-Chain Operations	18
12	Mimoto's Role in the Future ICAM Environment	19
13	Conclusion	19

Executive Summary

Zero Trust has moved from architectural aspiration to operating standard. Across the private sector, critical infrastructure, and government, organizations have made sustained investments in Identity, Credential, and Access Management (ICAM), endpoint security, network segmentation, data classification, and continuous monitoring. Those investments have materially strengthened security posture and brought the enterprise closer to the vision articulated in NIST SP 800-207 and the CISA Zero Trust Maturity Model: never trust, always verify.

Despite these advances, a fundamental challenge remains unresolved:

How can an organization continuously ensure that the individual operating under an authenticated identity remains the legitimate, authorized user throughout a session?

Traditional ICAM capabilities verify users at the point of authentication. Multifactor authentication, hardware-backed credentials, and federated identity services establish strong assurance that the right person is present at login. But from that moment forward, the architecture verifies the artifacts of identity (tokens, tickets, assertions, device posture) rather than the person. Increasingly sophisticated adversaries have adapted accordingly, shifting their focus to the period after authentication. Stolen credentials, hijacked sessions, insider access, and compromised endpoints all exploit the same structural weakness: once trust is granted, it is rarely re-examined.

Nation-state adversaries exploit this weakness most effectively. Their tradecraft is built around operating inside valid, authenticated sessions for months at a time while looking exactly like the legitimate user. Every point-in-time control has already been satisfied by the time they act, and threshold-based analytics are designed to catch spikes that disciplined operators never produce. Catching this class of adversary requires verification that continues for the duration of every session, measuring not whether the credential is valid, but whether the person behind it is who the credential claims.

The leading Zero Trust frameworks have already recognized this. NIST SP 800-207 describes trust as something continually evaluated rather than granted once, and the CISA Zero Trust Maturity Model defines its highest stage of identity maturity as

continuous verification of identity, not just when access is initially granted, with identity risk determined in real time. The mandate exists. What most environments lack is a capability that fulfills it.

Continuous Identity Assurance addresses this gap by extending identity verification beyond the login event and throughout the duration of user activity. By integrating behavioral analytics and dynamic trust assessments into existing Zero Trust architectures, organizations can strengthen resilience against credential-based attacks while maintaining operational effectiveness. Identity ceases to be a static, point-in-time event and becomes a continuously evaluated security signal, one that feeds risk-based access decisions, automated response, and enterprise analytics.

Mimoto provides a Continuous Identity Assurance capability designed to augment, not replace, existing ICAM investments and to advance Zero Trust maturity on the timeline each organization has set. This paper identifies the specific points at which current Zero Trust implementations stop verifying that the right person is present, describes the threat landscape that exploits those gaps (with particular attention to nation-state tradecraft), and explains how Continuous Identity Assurance maps to the pillars of Zero Trust and the maturity outcomes the leading frameworks define.

02

The Identity Gap in Zero Trust

Zero Trust rests on three foundational principles:

THREE PRINCIPLES

1 Verify explicitly

2 Use least privilege access

3 Assume breach

Most current identity architectures satisfy the first principle at a single moment in time: the authentication event. Multifactor authentication, hardware-backed credentials, federation services, and enterprise identity providers establish a high degree of trust at the beginning of a session. That trust is then encoded into a token, a ticket, or a session cookie, and from that point forward, the session artifact, not the human being, is what systems actually verify.

This creates a subtle but consequential inversion of Zero Trust principles. Trust established at authentication may persist long after the underlying assumptions supporting that trust have changed. The credential may have been phished. The token may have been stolen. The workstation may have been left unattended. The

user's intent may have changed. In each case, the session continues to operate with full authority because nothing in the architecture is responsible for asking the question again.

Questions that remain difficult for most current architectures to answer include:

- Has the authenticated account been compromised since login?
- Has the session been transferred to another individual?
- Is an insider misusing access they were legitimately granted?
- Has a privileged account been hijacked mid-session?
- Has the operational risk associated with a user increased since access was granted?

Without continuous reassessment, organizations risk extending exactly the kind of implicit trust that Zero Trust architectures were explicitly designed to eliminate. The gap is not a failure of existing ICAM investments. It is a boundary of their design scope. Closing it requires a capability purpose-built for the post-authentication period.

Where Zero Trust Stops Asking "Is It the Right Person?"

The Zero Trust model is rigorous about *what* is connecting (the device, the network path, the application, the data classification) and comparatively silent about *who* is actually present once a session is underway. The gaps are not abstract. They occur at specific, identifiable points in the architecture:

Authentication proves possession, not presence.

A smart-card or security-key login proves that someone holds the device and knows the PIN. An MFA push proves that someone approved a prompt. Neither proves that the same individual is at the keyboard five minutes, or five hours, later. From the authentication event forward, the architecture infers identity rather than observing it.

Session artifacts carry identity forward unexamined.

Tokens, tickets, and cookies encode the authentication decision and re-present it to every downstream system. Token lifetimes are typically measured in hours or days, and refresh mechanisms routinely extend sessions without any renewed check on the human. Whoever holds the artifact *is* the user, as far as the architecture is concerned.

Policy engines evaluate attributes, not people.

Policy decision points weigh device posture, location, time of day, resource sensitivity, and user role. But the "user" input to that calculation is simply whatever the token asserts. Risk-based access, as commonly implemented, is context-based access. It can detect that a session is coming from an unusual place; it cannot detect that a session is being driven by an unusual person from a usual place.

Device health is mistaken for user legitimacy.

Comprehensive device compliance (patched, encrypted, managed, EDR-enabled) is treated as strong evidence that access should continue. A fully compliant device operated by an unauthorized individual passes every device-pillar check the architecture can perform.

Step-up authentication is triggered by events, not by identity drift.

Re-authentication is commonly demanded on a timer, on a change of location or device, or on request for a designated high-value resource. A patient adversary who stays within the compromised user's normal footprint and avoids actions that draw attention is never challenged, which is precisely the behavior sophisticated actors exhibit.

Privileged access is checked at the vault door, not during the session.

Privileged access management solutions strongly govern the checkout of administrative credentials. Once a privileged session is open, however, the architecture has no continuing basis to confirm that the administrator who checked out the credential is the one exercising it.

Federation imports another authority's point-in-time decision.

In partner, subsidiary, and supply-chain environments, the enterprise accepts an identity assertion issued by another organization's identity provider. That assertion reflects a login event elsewhere, under policies the receiving organization may not control and cannot re-verify.

Walk-away and shared-terminal scenarios generate no signal.

A card left in a reader, an unlocked console in an operations center or trading floor, a virtual desktop session left open: in each case, the architecture has no mechanism to detect that the authenticated user has departed and someone else has assumed their seat.

Human accounts increasingly carry non-human operators.

Scripts, automation, and AI agents run under human credentials with growing frequency. The architecture sees a valid user account behaving in a permitted way. It has no native means of determining whether a person or a process is behind it.

Each of these gaps shares a single root cause: the architecture verifies the artifact of identity (a credential, a token, an assertion) rather than the person the artifact is supposed to represent. Every other pillar of Zero Trust has moved to continuous evaluation. The human element has not. That asymmetry is the identity gap, and it is the gap Continuous Identity Assurance is built to close.

03

The Frameworks Already Call for It

Continuous Identity Assurance is not a capability searching for a mandate. The two frameworks that define Zero Trust for most organizations, NIST Special Publication 800-207 and the CISA Zero Trust Maturity Model, both describe continuous evaluation of the user as a required characteristic of a mature architecture, and both treat the single-authentication model that most environments still operate today as a starting point rather than a destination.

NIST SP 800-207: Zero Trust Architecture.

NIST's foundational publication frames Zero Trust as a continuous cycle: obtain access, assess threats, adapt, and continually re-evaluate the trust extended to every subject. Among its core tenets, access to resources is to be determined by dynamic policy that includes the observable state of the requesting identity and may incorporate behavioral and environmental attributes; all authentication and authorization is to be dynamic and strictly enforced; and the enterprise is to collect as much information as possible about the current state of its subjects and assets and use it to improve access decisions. Nothing in that model is satisfied by a decision made once at login and carried forward on a token.

CISA Zero Trust Maturity Model: Identity pillar.

The maturity model makes the progression explicit. In the Authentication function, the Traditional stage authenticates identity with passwords or MFA and static access; the Initial and Advanced stages move to phishing-resistant MFA and verification of multiple entity attributes; and the Optimal stage is defined as continuously verifying identity, not just when access is initially granted. In the Risk Assessment function, the Optimal stage determines identity risk in real time based on continuous analysis and dynamic rules. The model's cross-cutting Visibility and Analytics and Automation and Orchestration capabilities are likewise expected, at maturity, to draw on continuous behavioral signals and to enforce policy dynamically in response to them.

What the frameworks share.

Both describe an end state in which trust is a live quantity that rises and falls with observed conditions, in which authentication is an ongoing process rather than a gate, and in which policy engines act on behavioral and contextual telemetry about the user rather than on a static assertion. Both also place the enterprise's most consequential trust decision, who is present, on the same footing as device compliance, network segmentation, and data protection, all of which are already evaluated continuously.

The practical significance is this: the frameworks have already made the determination that point-in-time authentication is insufficient, and have written continuous verification of identity into their definition of maturity. What remains is a capability gap, not a policy gap. Most ICAM stacks deployed today can satisfy the Traditional through Advanced stages of the identity pillar. Very few can deliver what the Optimal stage describes: sustained, behavior-informed confidence that the authenticated human is still the one present. Continuous Identity Assurance is a direct answer to that requirement.

04**Emerging Threats to Identity Assurance**

Adversaries have learned that the most efficient path into a well-defended environment is not to break the perimeter but to become a trusted user. Four threat categories illustrate how the post-authentication gap is exploited in practice.

Credential Compromise

Stolen credentials remain one of the primary vectors used by sophisticated adversaries, including nation-state actors targeting enterprise and critical infrastructure networks. Common attack methods include:

- Phishing and spear-phishing campaigns
- Adversary-in-the-middle attacks that intercept authentication flows
- Credential-harvesting malware
- Push-fatigue attacks against MFA systems
- Theft and replay of authentication tokens

Once authenticated, adversaries inherit the same permissions as the legitimate user they are impersonating. From the perspective of downstream systems, nothing is wrong: the credential is valid, the token is signed, the policy checks pass. Traditional ICAM systems lack the mechanisms necessary to distinguish between the authorized individual and an unauthorized actor operating under valid credentials, because the credential, not the person, is what they were built to evaluate.

Insider Threat

Insiders possess legitimate access to systems, networks, and sensitive information, which places them beyond the reach of controls designed to keep unauthorized actors out. While the overwhelming majority of users act responsibly, malicious or negligent insiders can create substantial operational risk, and history demonstrates that the damage from a single trusted insider can be severe and enduring.

Behavioral indicators of emerging insider risk may include:

- Unusual access patterns relative to established baselines
- Unexpected utilization of elevated privileges
- Deviations from normal workflows and working patterns
- Access to atypical information repositories
- Changes in operational behavior over time

Continuous Identity Assurance introduces additional signals that help organizations identify emerging insider threats before damage occurs, shifting insider-threat detection from after-the-fact forensics toward real-time risk awareness.

Account Takeover

Account takeover occurs when an unauthorized individual gains control over an existing user account, whether through credential theft, social engineering of help-desk processes, or exploitation of account-recovery mechanisms. Because authentication has technically succeeded, many security systems fail to recognize the compromise until after damage has occurred.

Dynamic identity assessment changes this calculus. When identity confidence degrades mid-session, organizations can adapt their defensive posture in real time rather than waiting for an incident report. Potential responses include:

- Step-up authentication challenges
- Privilege reduction
- Increased monitoring and telemetry capture
- Conditional access restrictions
- Session termination

Critically, these responses can be proportional. A modest drop in confidence might trigger silent monitoring; a severe anomaly might terminate the session outright. Proportionality preserves productivity for legitimate users while constraining adversaries.

Session Hijacking

Modern adversaries increasingly target authenticated sessions rather than the credentials themselves. It is a rational adaptation, since strong MFA has raised the cost of credential theft while session artifacts often remain comparatively unprotected. Examples include:

- Session token replay
- Browser cookie theft
- Man-in-the-browser attacks
- Compromise of remote access and virtual desktop environments

These attacks exploit the same structural fact: identity verification ceases once authentication has been completed. A stolen session is, from the system's point of view, indistinguishable from the original one. Persistent identity verification restores the missing check, maintaining confidence that the authorized individual, not merely the authorized session artifact, remains present throughout the session.

Nation-State Adversaries: Why Point-in-Time Verification Fails

The four threat categories above are exploited by a wide range of actors. Nation-state adversaries, however, combine them in ways that expose the limits of point-in-time verification most starkly, and their target list has expanded well beyond government. Critical infrastructure operators, financial institutions, technology and cloud providers, healthcare systems, and any organization that sits in a government or defense supply chain are now routine targets.

How Nation-State Actors Operate Inside Defended Networks

Publicly reported intrusions against enterprise, critical infrastructure, and government networks over the past several years share a consistent pattern: the adversary does not break in, they log in. State-sponsored campaigns have repeatedly favored valid accounts over malware, harvesting or purchasing credentials, intercepting authentication flows to defeat MFA, stealing and replaying session tokens, abusing federation and OAuth trust relationships, and recruiting or coercing insiders. Once inside, they "live off the land," using the same administrative tools, remote access paths, and cloud consoles that legitimate users rely on every day.

Several characteristics distinguish this class of adversary from opportunistic attackers:

Patience.

Nation-state operations are measured in months and years, not hours. Dwell times of several months before discovery are routine in public reporting. The objective is durable access and quiet collection, not rapid monetization.

Discipline.

Operators work within the compromised user's normal working hours, touch resources the user plausibly needs, and avoid actions that trigger alerts. Their operational security is designed specifically to defeat threshold-based detection.

Resources.

Well-funded programs can afford to acquire zero-day access, purchase credentials at scale, run adversary-in-the-middle infrastructure, and now deploy AI agents to automate reconnaissance, phishing, and lateral movement at speed.

Strategic focus.

The target is not the account; it is what the account can reach: intellectual property, operational technology, customer and personnel data, financial systems, and the trust relationships that connect the organization to its partners and customers.

Why Current Zero Trust Implementations Miss Them

Against this adversary, every point-in-time control the architecture depends on has already been satisfied. The credential is valid. The MFA challenge was passed, or bypassed at the moment it was issued. The device is compliant, because it is the legitimate user's device. The session originates from an expected location during expected hours. The policy engine sees a known user doing permitted things.

The architecture's implicit assumption is that anomalous behavior will look anomalous. Nation-state tradecraft is built on the opposite premise: look exactly like the user. A disciplined operator working inside a legitimate account generates no failed logins, no impossible travel, no privilege escalation alerts, and no malware signatures. From the perspective of a Zero Trust stack that verified identity once and then moved on, there is nothing to find.

This is the central problem: point-in-time verification catches adversaries who are careless at the moment of login. Nation-state adversaries are not careless, and they do not need to defeat the login. They need only to survive it.

What Continuous Assurance Changes

Continuous Identity Assurance inverts the advantage. Rather than looking for the adversary's mistakes, it measures the adversary's inability to be someone else.

The baseline is the person, not the account.

An account's permissions, schedule, and typical resources can be studied and imitated. The way a specific individual interacts with systems (the accumulated behavioral signature built over weeks of legitimate use) cannot be harvested from a credential dump or observed from outside the session. An operator working under a stolen identity is, by definition, not that identity, and the divergence is measurable.

Time becomes the defender's asset.

In a point-in-time model, every additional day of undetected access strengthens the adversary's position. Under continuous assurance, every additional action is another verification event. A campaign designed for a multi-month dwell time must sustain a behavioral impersonation for that entire period, a burden that grows heavier with each session rather than lighter.

Low-and-slow is exactly what it detects.

Threshold-based analytics look for spikes. Continuous identity confidence looks for drift: the gradual, sustained deviation from an individual's established pattern that disciplined operators produce precisely because they are avoiding spikes.

Insider recruitment is addressed by the same mechanism.

When a nation-state actor coerces or recruits a legitimate user, the credential and the person match, but the behavior changes. Access to unfamiliar repositories, altered working patterns, and unusual data handling surface as identity-confidence signals, not as authentication failures.

The evidentiary record supports investigation, not just response.

A continuous, quantified identity signal produces a session-by-session record of confidence over time. When a compromise is identified, that record shows when the impersonation began, which sessions were affected, and what the adversary reached: the questions incident response, legal, and regulatory teams must answer and that point-in-time logs cannot.

Zero Trust's third principle is "assume breach." Against the actors most capable of breaching the enterprise, assuming breach means assuming that a valid, authenticated, MFA-verified session may be adversary-controlled, and building a capability to test that assumption continuously, for the duration of every session, without imposing friction on the legitimate workforce. That is the function Continuous Identity Assurance performs, and it is the reason the Optimal stage of identity maturity cannot be reached with authentication-time controls alone.

06

Continuous Identity Assurance

Continuous Identity Assurance extends identity verification throughout the session lifecycle. Rather than relying exclusively upon a single authentication event, it evaluates identity confidence over time using multiple contextual indicators, including:

- Behavioral characteristics unique to the individual
- Interaction patterns with systems and applications

- Operational context of the activity being performed
- Environmental attributes of the device and connection
- Historical usage profiles built over time

These signals are combined into a dynamic identity confidence assessment that evolves as the session progresses. When observed behavior remains consistent with the authenticated identity, the session proceeds without friction, and legitimate users experience no interruption. When deviations occur, organizations can employ adaptive responses aligned with business priorities and risk tolerance, from silent escalation of monitoring to immediate session termination.

The result is a fundamental shift in how identity functions within the architecture:

Continuous Identity Assurance transforms identity from a static event into a dynamic security signal.

This shift aligns identity with how Zero Trust treats every other element of the environment. Networks are continuously monitored. Devices are continuously assessed for compliance. Data is continuously tagged and tracked. Identity, arguably the most consequential trust decision in the architecture, should be held to the same standard.

07

Agentic Zero Trust Attacks: Two Questions, One Architecture

The rise of agentic AI introduces a new dimension to the identity challenge. Agentic attacks target Zero Trust with multiple approaches: autonomous agents can now conduct reconnaissance, phish credentials, hijack sessions, and operate inside authenticated environments at machine speed, and increasingly, they defeat the legacy defenses designed to keep automation out. The defense is two questions, both of which must be answered continuously.

"Is this a human?" Human verification distinguishes agents from humans, stopping automation that now passes legacy CAPTCHA and behavioral checks. As agentic tools become more capable of mimicking human interaction patterns, point-in-time bot detection, like point-in-time authentication, loses its protective value. The determination must be sustained across the session.

"Is it the right human?" Continuous Identity Assurance answers the second question: knowing which specific human is present, verified continuously through the session rather than once at login. Together, the two questions form a single identity architecture, one that addresses both the automation threat and the impersonation threat without gaps between them.

Critically, this architecture does not force an enforcement model on the enterprise. Organizations can apply rules natively (challenging, restricting, or terminating sessions directly) or feed real-time identity signals into the existing SIEM, ICAM, and policy enforcement stack. Enforce or signal: the choice rests with the organization, and either path builds on the infrastructure already in place.

08

Supporting the Pillars of Zero Trust

The leading Zero Trust frameworks organize their capability models around a common set of pillars (identity, devices, applications and workloads, data, and network), supported by cross-cutting visibility, analytics, automation, and orchestration. Continuous Identity Assurance contributes directly to each of them, with the deepest impact concentrated in the identity pillar and cascading benefits across the remainder of the model.

Identity

Continuous verification strengthens confidence that authenticated users remain legitimate throughout their activity: the central outcome the identity pillar exists to achieve. Contributions include:

- Stronger identity confidence throughout the session
- Detection of account misuse and impersonation
- Adaptive and risk-based authentication support
- Continuous user verification aligned with Optimal-stage maturity outcomes

Devices

Device trust and user trust are interdependent: a compliant, healthy device operated by the wrong person is still a compromised asset. Behavioral indicators can identify inconsistencies suggesting that trusted devices are being operated by unauthorized individuals. Combining user-identity confidence with device-posture assessment produces a unified risk picture that neither signal provides alone.

Applications and Workloads

Identity confidence can inform application access decisions at a granular level. Applications may dynamically adjust permissions (restricting sensitive functions, requiring re-verification for high-impact transactions, or degrading gracefully to read-only access) based upon evolving trust conditions rather than a single decision made at login.

Data

Continuous Identity Assurance supports data-centric security by helping ensure that the individuals accessing sensitive information remain authorized throughout the interaction, not merely at the moment access was granted. For an organization's most sensitive data holdings, the difference between point-in-time and persistent assurance is the difference between trusting a session and trusting a person.

Network

Behavioral anomalies associated with authenticated sessions provide additional signals relevant to network defense activities, enriching segmentation and access decisions with identity context. Identity becomes an operational input supporting environmental awareness rather than an isolated function.

Automation and Orchestration

Identity confidence signals serve as high-value triggers for automated response. Because the signal is continuous and quantified, it integrates naturally with orchestration platforms to drive:

- Conditional access enforcement
- Session restrictions and step-up challenges
- Dynamic privilege adjustments
- Security operations and SOAR workflows

Visibility and Analytics

Continuous Identity Assurance generates valuable telemetry supporting enterprise monitoring, threat hunting, and risk analysis. Identity itself becomes a continuously monitored indicator: a data stream that analysts can correlate with endpoint, network, and data-layer telemetry to see attacks that no single layer would reveal.

Alignment with Zero Trust Maturity Outcomes

The leading Zero Trust frameworks emphasize outcomes associated with risk-based access decisions, continuous verification, dynamic policy enforcement, integrated security telemetry, and automated response mechanisms. Continuous Identity Assurance contributes to these outcomes through four mutually reinforcing capabilities:

Enhanced Verification.

Identity verification persists beyond authentication events, operationalizing the “never trust, always verify” principle for the human element of the architecture.

Dynamic Trust Evaluation.

User confidence levels evolve based upon observed conditions, giving policy engines a live risk signal rather than a stale point-in-time attestation.

Improved Threat Detection.

Credential misuse and session anomalies become visible during the attack, when intervention is still possible, rather than after the fact.

Adaptive Security Response.

Security controls respond proportionally to changing risk conditions, preserving productivity for legitimate users while constraining adversaries.

Together, these capabilities directly support the Optimal stage of identity maturity by supplying the continuous, user-focused verification that the frameworks' most advanced outcomes presuppose. They map most directly to the Authentication and Risk Assessment functions of the identity pillar and to the behavioral-analytics expectations of the cross-cutting Visibility and Analytics capability, allowing organizations at the Initial or Advanced stage to reach Optimal-stage identity outcomes without waiting for every other pillar to catch up.

Integration Within Existing ICAM Ecosystems

Continuous Identity Assurance is not intended to replace existing ICAM capabilities. Organizations have made substantial, well-founded investments in enterprise identity infrastructure, and those investments remain the foundation of the identity architecture. Continuous Identity Assurance enhances:

- Enterprise identity providers

- Smart-card, security-key, and certificate-based credential infrastructures
- Federation services
- Multifactor authentication systems
- Conditional access engines
- Security information and event management (SIEM) platforms

Mimoto is designed to function as an identity assurance layer operating alongside existing architectures, consuming authentication context from the systems already in place and returning continuous identity confidence to the policy engines, applications, and analytics platforms that can act on it. This approach minimizes disruption, avoids rip-and-replace costs, and increases resilience against emerging threats without requiring changes to the credentials or workflows users already know.

11

Enabling Partner, Subsidiary, and Supply-Chain Operations

Multi-organization environments introduce identity challenges that strain traditional approaches. Partners, subsidiaries, contractors, and suppliers rely upon different credentialing systems, identity authorities, and security policies, and traditional identity architectures often struggle to establish consistent trust relationships across these organizational boundaries. The result is a familiar tension: either access is impeded and collaboration suffers, or trust is extended on the basis of assurances that cannot be independently verified.

Continuous Identity Assurance offers a path through this tension. Because persistent verification operates independently of the originating credential source, it provides a consistent, observable basis for trust in shared environments, regardless of which organization issued the underlying credential. Potential use cases include:

- Joint ventures and shared operating environments
- Post-merger integration before identity systems are consolidated
- Contractor and managed-service-provider access
- Supply-chain and B2B portals
- Multi-tenant platforms and shared development environments

In each case, the value proposition is the same: confidence in who is operating within the shared environment right now, sustained continuously, without requiring partners to harmonize their credentialing infrastructures first.

12

Mimoto's Role in the Future ICAM Environment

As organizations modernize ICAM capabilities and expand Zero Trust implementation toward the Optimal stage of maturity, Continuous Identity Assurance offers a complementary capability designed to strengthen, and extract greater value from, identity investments already made. Mimoto supports the transition from:

Point-in-time authentication



Persistent identity confidence

By continuously verifying that authenticated users remain legitimate throughout their activity, organizations improve protection against the full spectrum of post-authentication threats:

- Credential compromise
- Insider threats
- Account takeover
- Session hijacking
- Unauthorized privilege utilization

Continuous Identity Assurance provides a practical, non-disruptive mechanism for advancing Zero Trust objectives while preserving the operational effectiveness that the business requires.

13

Conclusion

Organizations have made substantial progress toward implementing Zero Trust architectures. But adversaries have adapted, and they increasingly target the period after authentication, exploiting the persistence of trust granted through legitimate credentials. The nation-state actors most capable of harming an enterprise no longer need to defeat the login; they need only to survive it, and current architectures give them every opportunity to do so undetected. Reaching a mature Zero Trust posture requires extending identity verification beyond login events and integrating continuous assurance into operational environments.



The future of identity security lies not only in determining who entered the system, but in continuously verifying who remains inside.

Continuous Identity Assurance represents an important evolution in protecting an organization's people, operations, and information in an increasingly contested digital environment. Mimoto is committed to delivering that capability in partnership with its customers, building on the ICAM foundation already in place and closing the identity gap that stands between today's architectures and true Zero Trust.

For more information: mimoto.ai/contact

ABOUT MIMOTO

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

Mimoto provides person-based continuous verification for the AI agentic era. It checks, all session long, that the person in a session is real and is the right person, and catches stolen credentials, hijacked sessions, and impersonation by people or AI agents while they are happening.

See where the gap sits in your environment.

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