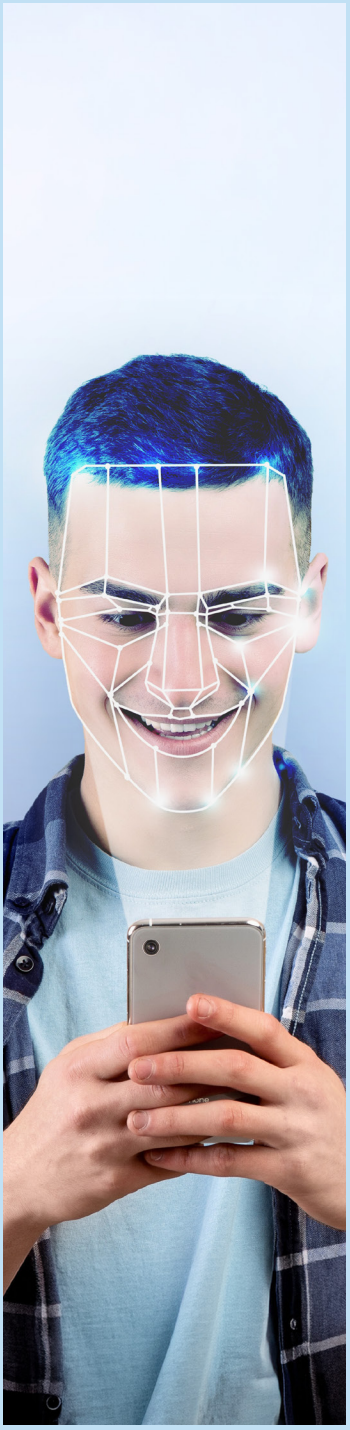
VIEW POINT



BIOMETRIC AUTHENTICATION TRENDS: STRENGTHENING USER ACCOUNT SAFETY IN 2026

Abstract

Biometric authentication is evolving from a convenience feature into a strategic enterprise control. In 2026, organisations are strengthening user account safety through biometric passkeys, advanced Presentation Attack Detection (PAD), behavioural biometrics, crypto-agile architectures, and privacy-preserving template protection. At the same time, boards are demanding measurable risk reduction, regulatory compliance, and ethical design aligned with Industry 5.0 principles. This article explores ten key trends shaping the future of identity assurance, from post-quantum readiness and multi-sensor anti-spoofing to user trust and change management. It outlines how enterprises can reduce fraud exposure, improve user experience, and build resilient authentication ecosystems that balance security, transparency, and long-term business value.

Infosys®
Navigate your next

As traditional credential boundaries dissolve, identity is becoming the primary security perimeter.

Passwords are phished. Tokens are intercepted. Access cards are cloned. Traditional credentials, designed for a simpler digital era, have become both operational burdens and security liabilities.

Enterprises are now embracing a fundamentally different model. Instead of relying on what users know or carry, leading organisations are building identity ecosystems around biometric authentication. Identity is becoming adaptive, data-driven, and anchored in the individual rather than in vulnerable artefacts.

This transformation is unfolding against a backdrop of rising fraud, regulatory scrutiny, post-quantum preparedness planning, and Industry 5.0's emphasis on human-centric resilience. Boards now demand measurable risk reduction, not incremental security upgrades.

Biometrics, when implemented responsibly and strategically, offer durable trust. The following trends explore how biometric authentication is strengthening user account safety through technology, smarter governance, quantifiable risk reduction, and human-centred design.

1. Biometric passkeys move from innovation to enterprise standard

Enterprises are steadily moving toward biometric-based passkeys as the standard method for passwordless authentication. Unlike traditional passwords, passkeys use public-key cryptography that is tied to a secure device component (such as a secure enclave or Trusted Platform Module) and unlocked using biometrics verified locally on the device. Because servers do not store biometric data or reusable secrets, the risk of credential theft and phishing is greatly reduced.

Passkey adoption will increase across web applications, consumer platforms, and enterprise identity and access management systems. This growth is driven by industry standardisation and user expectations for simple but secure login experiences. As adoption rises, organisations can expect fewer credential-related breaches and improved user satisfaction. Biometric passkeys are increasingly viewed as a core layer in modern identity architecture.

Enterprise implications:

- Make passkeys the default authentication method for users and administrators.
- Implement device attestation and revocation processes for lost or replaced authenticators.

2. Presentation attack detection evolves into multi-sensor security

Presentation attacks, where attackers use spoof materials such as masks, printed photos, or deepfake videos, are becoming more advanced and harder to detect. In 2026, Presentation Attack Detection (PAD) will move from static checks to dynamic, multi-sensor defence systems. These solutions combine micro-movement analysis, 3D depth detection, infrared sensing, and AI-based anti-spoofing models to confirm that a real person is interacting with a genuine sensor.

Regulatory and standards organisations are defining clear PAD benchmarks, making anti-spoofing a formal requirement in high-assurance systems.

Enterprise implications:

- Require ISO-aligned PAD testing evidence in procurement contracts.
- Deploy multi-sensor PAD controls for high-risk processes such as account recovery and privileged access.

3. Behavioural biometrics bring an era of frictionless security

Behavioural biometrics analyse how users interact with devices and systems, including typing rhythm, touch gestures, and mouse movements. These signals will soon form a continuous risk assurance layer that quietly checks session legitimacy in real time. Instead of being a one-time check, behavioural signals allow ongoing monitoring during a session.

When combined with device integrity data and network risk scores, behavioural telemetry can adjust risk levels and trigger adaptive authentication only when needed.

This approach improves user experience by reducing unnecessary friction while maintaining strong security. The industry is developing adaptive human-computer interaction models that respond dynamically to behavioural and contextual signals, in line with Industry 5.0's focus on human-centred design.

Enterprise implications:

- Integrate behavioural signals into risk engines to support step-up authentication decisions.
- Use explainable scoring models to support governance and audit requirements.

4. Biometric security for a privacy-first world

As biometric use increases, privacy regulations are also expanding globally. Biometric templates, mathematical representations of biometric traits, must be stored and processed securely. Enterprises will widely adopt template protection methods such as cancellable biometrics, biometric shielding, and Secure Multiparty Computation (SMPC). These techniques ensure raw biometric data is not stored in readable form on central servers.

Many systems will also perform biometric matching directly on user devices or within trusted execution environments to reduce central exposure. This approach supports privacy-by-design principles required in many jurisdictions.

Enterprise implications:

- Make template protection capabilities mandatory in vendor evaluations.
- Review retention policies to align biometric data with privacy and residency requirements.

5. Crypto-agile biometric authentication for quantum-ready security

Post-quantum cryptography is steadily becoming a part of the ecosystem. Organisations must plan for it now. Cryptographic components within identity systems, including biometric passkey key pairs and authentication assertions, must be crypto-agile. This ensures support for emerging post-quantum algorithms without requiring disruptive user re-enrolment.

Forward-looking enterprises will adopt hybrid cryptographic stacks that support both classical and post-quantum algorithms. This enables smooth migration when standards stabilise. A proactive approach protects biometric authentication systems from future cryptographic weaknesses.

Enterprise implications:

- Map cryptographic dependencies across identity systems.
- Select authenticators that support flexible, hybrid upgrade paths.

6. Biometric risk quantification becomes a priority

Biometric authentication will henceforth be viewed as a technical security control and a measurable business risk management tool. Risk mitigation demands clear evidence that biometric investments reduce fraud, prevent breaches, and lower operational costs.

Instead of reporting only technical metrics such as false acceptance rates, organisations will link biometric performance to financial outcomes. These may include fraud loss reduction, fewer helpdesk resets, lower insurance exposure, and improved compliance posture. This shift helps security leaders align identity strategy with enterprise risk frameworks.

Enterprise implications:

- Build dashboards that connect biometric performance to financial risk reduction.
- Use quantitative risk models to demonstrate measurable value to executive stakeholders.

7. Advancing human-centric automation with workforce biometrics

Beyond securing user accounts, biometric authentication is becoming an important safety and trust layer within human-machine collaborative environments, a central focus of Industry 5.0. This new phase of industrial transformation prioritises human empowerment, safety, inclusion, and closer collaboration between people and intelligent systems.

In smart manufacturing, logistics, and healthcare settings, biometric systems will be used to verify operators, monitor signs of fatigue or stress, and control access to equipment based on role and real-time safety conditions. Biometrics will increasingly connect with edge AI and cyber-physical systems, supporting more context-aware and adaptive governance across complex, hybrid operational environments.

Enterprise implications:

- Design workflows that account for safety, ergonomics, and workplace context.
- Integrate identity signals with operational controls, such as machine lockouts when unsafe conditions are detected.

8. Ethical, accessible, and sustainable design becomes a core KPI

Industry and regulatory expectations are shifting toward ethical and accessible biometric solutions. Enterprises will be assessed not only on accuracy and security, but also on inclusive performance across diverse populations, energy efficiency, and lifecycle sustainability. Inclusion metrics, such as performance across different skin tones, age groups, and physical abilities, will increasingly appear in procurement scorecards and regulatory compliance attestations.

Sustainability factors, embedded in frameworks such as Industry 5.0 and ESG reporting standards, will require organisations to measure and report the environmental footprint of deployed biometric systems. This may include the impact of sensor manufacturing, energy consumption levels, and responsible end-of-life disposal practices.

Enterprise implications:

- Include inclusivity and sustainability criteria in vendor selection.
- Document accessibility testing to support governance and brand trust.

9. Shared threat intelligence for biometric attack patterns

Static defences are no longer effective in an environment shaped by advanced AI-driven attacks and synthetic identity threats. Industry consortia and cross-sector coalitions will share machine-readable biometric attack indicators, similar to cybersecurity threat feeds, so organisations can quickly update PAD models and behaviour classifiers.

This approach supports modern cyber risk strategies that focus on collaboration across organisations to detect and stop complex attacks. By sharing attack patterns, including deepfake techniques and adversarial manipulation methods, defenders can strengthen authentication systems before threats cause damage.

Enterprise implications:

- Participate in identity-focused threat intelligence communities.
- Integrate shared indicators into biometric risk engines.

10. Governance and compliance: Audit trails, explainability, and accountability

As biometric systems become more integrated into core business functions, they will face increasing regulatory scrutiny. Compliance will require strong auditability, clear explainability, interpretability, and defined human-in-the-loop processes. Automated biometric decisions, especially for high-risk actions, must include detailed logs that record triggers, confidence scores, and escalation steps.

Regulators and auditors are signalling that opaque, purely AI-driven authentication decisions will no longer meet governance standards. Systems must provide clear and interpretable evidence to explain outcomes, along with appeal mechanisms for users affected by automated denials or step-up authentication requests.

Enterprise implications:

- Implement structured logging to support audits.
- Define formal human oversight processes for high-impact decisions.

Beyond technology: Building trust in biometric system

Advanced biometric systems will not succeed without user trust. Organisations must focus on technical performance, transparency, and clear communication. Employees and customers want to understand how their biometric data is stored, protected, and used.

Clear explanations of template protection, data retention, and revocation rights help address concerns.

Consent processes must be simple and visible. Users should know when biometric data is captured and for what purpose. Over half of users now rely on biometric methods for daily authentication, indicating strong momentum toward widespread adoption.

However, privacy and control of personal data are very important when deciding whether to use biometric authentication or identity systems.

Change management is also critical. Moving from passwords to biometric passkeys affects workflows and user behaviour. Structured onboarding, training, and phased rollouts can reduce resistance.

Biometric authentication is now a trust strategy, and organisations that combine strong safeguards with transparent communication will achieve faster adoption and greater long-term value.

Toward identity assurance 2.0

Biometric authentication will soon evolve into a strategic enterprise capability shaped by trust, governance, and measurable risk outcomes. Organisations embracing crypto-agility, behavioural assurance, and ethical design will better secure users and operations. Combined with multi-layer trust signals and inclusive governance, biometrics will shift identity from a reactive checkpoint to a continuous assurance engine aligned with business and regulatory priorities.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next