

Controlling Identity-Based Threats: Debunking Myths and Misconceptions

Author: Todd Thiemann

October 2026

In partnership with:



Contents

Executive summary	4
The evolution from identity verification to identity threat detection	4
The business impact of identity threats and incorrect trust decisions	6
Essential definitions	7
Identity security myths and misconceptions.....	8
Foundational misconceptions	9
Myth 1: Multifactor authentication (MFA) is an adequate control, and successful authentication is proof of identity.	9
Myth 2: A government ID plus a selfie provides identity.....	9
Myth 3: Liveness detection solves deepfakes and impersonation.....	9
Myth 4: Successful identity verification means the person is not a threat.	10
Myth 5: Sending one-time passcodes (OTPs) via SMS/text or email provides sufficient security.....	10
Lifecycle and control misconceptions	10
Myth 6: We only need to verify identity once, at onboarding.	10
Myth 7: Strong controls at authentication give us robust identity security.	11
Myth 8: Strong MFA makes identity verification unnecessary.....	11
Myth 9: Account recovery is a customer service or help desk process, not an identity security event.	11
Customer experience and privacy misconceptions	12
Myth 10: More verification friction automatically means better security.	12
Myth 11: Low friction means weak security.	12
Myth 12: Collecting more personal data always improves identity security.	12
Architecture and strategy misconceptions	12
Myth 13: HR or CRM is already the source of truth, so additional identity controls are redundant.....	12
Myth 14: Identity security performance stays reliable once the program is deployed..	13
Myth 15: AI agents are primarily an application or data security issue.	13

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

Continuous identity threat detection delivers better outcomes	14
Appendix	15
Methodology	15
Further reading	15



Executive summary

While CISOs and security teams increasingly recognize that identity lies at the root of many enterprise data compromises and digital fraud incidents, efforts to combat identity-based attacks are often undermined by persistent myths and misconceptions. This paper helps identity and security leaders separate myths from reality, reduce identity threat exposure, and mitigate cyber risk by adopting a comprehensive identity threat detection strategy designed to identify and respond to identity-based attacks across the entire identity lifecycle.

The evolution from identity verification to identity threat detection

Many cybersecurity leaders are familiar with identity verification, particularly in the context of customer and consumer use cases. For example, financial institutions have long relied on identity verification to support Know Your Customer (KYC) and Anti-Money Laundering (AML) regulatory requirements.

However, identity risk now extends well beyond these traditional use cases. Interest in identity threat detection has grown significantly as changes in how and where people work, combined with high-profile identity-based attacks, have elevated identity risk to a board-level concern.

The enterprise identity-risk landscape has changed considerably with the growth of remote and hybrid work, increasing organizations' reliance on remote employee onboarding, third-party and contractor access, and distributed workforces. These changes make it increasingly important not only to verify an identity at onboarding but also to continuously assess whether that identity can still be trusted.

The same evolution is occurring across customer identity and access management (CIAM). Digital channels increasingly support self-service registration, account recovery, credential resets, payment changes, and other high-risk interactions. Establishing identity at a single point in time is no longer sufficient; organizations need the ability to detect changes in identity risk throughout the customer lifecycle.

Adversaries are actively exploiting this expanded identity attack surface. Stolen credentials, social engineering, account recovery abuse, impersonation, and other identity-based techniques enable attackers to exploit trusted identities and legitimate access mechanisms.

Recent incidents involving North Korean threat actors impersonating US technology workers to gain employment, generate revenue, and steal sensitive information—as well as the steady stream of compromises involving credential and account resets—have further elevated the issue. Organizations increasingly recognize that identity must be addressed continuously to reduce the likelihood of breaches, intellectual property theft, account takeover, and identity fraud.

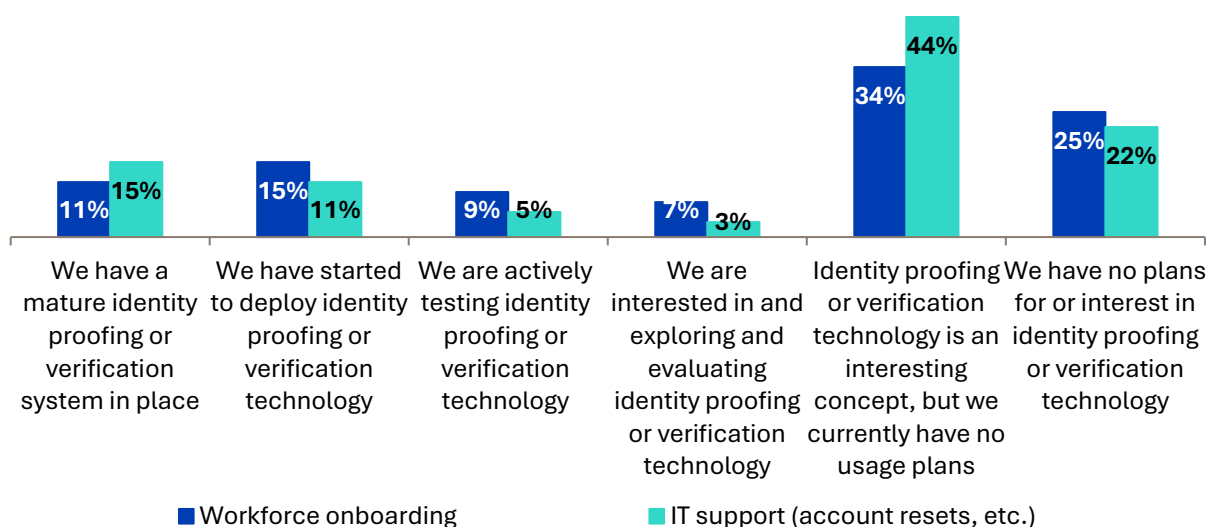
This is where identity threat detection represents the next stage of maturity beyond point-in-time identity verification. Rather than asking only whether someone can prove who they are during a specific digital interaction, identity threat detection continuously evaluates identity, device, credential, behavioral, and other risk signals to identify suspicious activity and enable an appropriate response.

Omdia research underscores the growing demand for these capabilities. While 26% of organizations have an identity proofing or verification system in place or being deployed, more than 50%, on average, are testing solutions or have expressed an interest in deploying them (see **Figure 1**).¹

¹ Source: Enterprise Strategy Group (now Omdia) Research Report, [Identity Security at a Crossroads: Balancing Stability, Agility, and Security](#), October 2025.

Figure 1: Workforce identity proofing verification implementation

What is your organization's usage status for identity proofing and/or verification in support of the following use cases? (Percent of respondents, n=369)



Source: Omdia

Interest in identity verification and identity threat detection is growing rapidly, but considerable confusion remains about their respective roles and capabilities. This paper addresses the most common myths and misconceptions, helping security and identity leaders understand the limitations of point-in-time identity verification and the value of a more comprehensive identity threat detection approach so they can make informed decisions about managing identity risk.

The business impact of identity threats and incorrect trust decisions

Identity risk does not end once an identity has been verified. A wrong identity or trust decision—whether during onboarding, authentication, account recovery, or an ongoing session—can create significant business risk. Organizations, therefore, need to look beyond individual identity and access management (IAM) control gaps and consider the financial, operational, regulatory, and reputational consequences of failing to detect identity threats throughout the identity lifecycle.

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

Table 1: The impact of identity risk

Impact	Workforce IAM examples	Customer IAM examples
Unauthorized access	An impersonator or fraudulent employee obtaining legitimate enterprise credentials and access	An attacker taking over a legitimate customer account or exploits compromised credentials
Financial loss	Payroll diversion, procurement fraud, intellectual property, or source-code theft	Account origination fraud, unauthorized payouts, promotion or refund abuse
Operational disruption	Fraudulent onboarding, help desk manipulation, account recovery abuse, remediation efforts	Increased abandonment, account lockouts, manual review burden, customer support costs
Regulatory risk	Inadequate access controls, weak auditability, failure to detect unauthorized access	KYC/AML failures, privacy violations, consumer protection concerns
Reputational damage	Publicized data breach, insider-like activity, or intellectual property theft originating from a compromised or fraudulent identity	Account takeover, compromised customer accounts, or legitimate customers incorrectly blocked

Source: Omdia

The business impact of identity threats demonstrates why point-in-time identity verification alone is insufficient. Organizations need **continuous identity threat detection** that evaluates risk throughout the identity lifecycle and enables security and fraud teams to detect and respond when the level of trust associated with an identity changes.

Essential definitions

Before examining the myths and misconceptions surrounding identity risk, it is important to establish a common vocabulary. The terms in **Table 2** distinguish between establishing identity, authenticating access, making risk decisions, and continuously detecting identity threats throughout the identity lifecycle.

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

Table 2: Key identity security definitions

Impact	Definition	Key question answered
Identity verification	Establishing that an individual is who they claim to be by validating identity evidence, attributes, and other relevant signals	Is this person who they claim to be?
Enrollment	Establishing the digital identity record or account and associating appropriate credentials and authenticators with it	How is this person represented and enabled within our systems?
Authentication	Verifying that an individual or entity controls the authenticator or credential associated with an identity	Does this person control the expected credential or authenticator?
Authorization	Determining what an authenticated identity is permitted to access or do	What is this identity allowed to access or do?
Fraud decisioning	Assessing whether a specific action or interaction is suspicious or potentially fraudulent	Should we allow, challenge, review, or block this activity?
Identity threat detection	Continuously evaluating identity, credential, device, behavioral, and other risk signals to identify suspicious activity, changes in trust, and potential identity-based attacks	Can we still trust this identity, and is its current activity consistent with legitimate use?
Friction	The additional time, effort, or inconvenience that a legitimate user experiences when establishing identity, authentication, or satisfying additional security controls	How much effort are we requiring from a legitimate user?
Identity lifecycle management	Managing identities, credentials, access privileges, role changes, and termination throughout their lifecycle	How should an identity and its access change over time?

Source: Omdia

Identity security myths and misconceptions

Many commonly held assumptions about identity security are rooted in point-in-time controls—verification, authentication, credentials, and individual transactions. While

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

these controls remain important, today's identity threats require organizations to continuously evaluate identity risk across the entire lifecycle.

The following myths and misconceptions highlight where traditional approaches can create gaps in identity trust, along with actions leaders can take to strengthen identity threat detection and reduce risk.

Foundational misconceptions

Myth 1: Multifactor authentication (MFA) is an adequate control, and successful authentication is proof of identity.

- **Reality:** MFA is an important authentication control, but successful authentication does not necessarily establish who is behind the credentials. MFA generally demonstrates control of the required authenticators. If credentials, devices, sessions, or recovery mechanisms have been compromised, an attacker may still successfully authenticate.
- **Leadership action:** Treat MFA as one layer of identity security, not proof of identity or continued trust. Combine strong authentication with identity verification and ongoing identity threat detection to evaluate whether the person, credentials, device, behavior, and activity remain consistent with a trusted identity.

Myth 2: A government ID plus a selfie provides identity.

- **Reality:** A government-issued ID, biometric comparison, and liveness detection provide valuable evidence and signals, but no individual signal eliminates identity risk. Stolen or manipulated documents, impersonation, synthetic identities, and other attack techniques can undermine point-in-time verification.
- **Leadership action:** Look beyond a single document-and-selfie check. Use multiple independent identity and risk signals and incorporate identity verification into a broader identity threat detection strategy capable of reassessing trust when risk changes.

Myth 3: Liveness detection solves deepfakes and impersonation.

- **Reality:** Liveness detection can help determine whether a live person is present during a digital interaction, but it does not, by itself, establish that the person is the rightful owner of the claimed identity, nor does it eliminate threats such as injection attacks, replay attacks, stolen identity evidence, or social engineering.

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

- **Leadership action:** Treat liveness as one signal within a layered identity security strategy. Combine biometric controls with identity, device, credential, behavioral, and other risk intelligence to detect attempts to circumvent individual controls.

Myth 4: Successful identity verification means the person is not a threat.

- **Reality:** Identity verification establishes confidence that someone corresponds to a claimed identity at a particular point in time. It does not establish that the individual has legitimate intent, nor does it protect against subsequent account compromise, credential theft, first-party fraud, insider-like activity, or changes in behavior.
- **Leadership action:** Do not allow a successful verification event to create permanent trust. Extend identity security beyond initial verification with continuous identity threat detection capable of identifying changes in risk throughout the identity lifecycle.

Myth 5: Sending one-time passcodes (OTPs) via SMS/text or email provides sufficient security.

- **Reality:** OTPs provide an additional authentication signal, but they are not proof of a real-world identity. Control of a phone number, device, session, or email account can change. Attackers increasingly combine social engineering, stolen personal information, SIM swapping, adversary-in-the-middle techniques, and session hijacking to circumvent OTP-based controls.
- **Leadership action:** Treat an OTP as evidence that someone currently controls a communication channel—not that the individual is necessarily the legitimate owner of the identity. Use OTPs within a layered approach that incorporates stronger authentication, identity verification, and identity threat detection.

Lifecycle and control misconceptions

Myth 6: We only need to verify identity once, at onboarding.

- **Reality:** Identity trust is static. Risk can change following onboarding and at critical events such as account recovery, credential resets, new device registration, profile changes, payroll updates, payment changes, privilege changes, and high-risk interactions.
- **Leadership action:** Move beyond a “verify once, trust indefinitely” model. Continuously assess identity risk and use adaptive verification or step-up controls when risk signals or sensitive events warrant additional assurance.

Myth 7: Strong controls at authentication give us robust identity security.

- **Reality:** Successful authentication establishes trust at a moment in time. It does not guarantee that the legitimate user, device, application, session, or intent remains trustworthy throughout the subsequent activity. Attackers can compromise sessions or exploit legitimate access after authentication.
- **Leadership action:** Extend identity threat detection beyond the authentication event. Continuously evaluate relevant identity, credential, device, behavioral, session, and transaction signals, and adapt controls when risk changes rather than allowing trust to persist indefinitely.

Myth 8: Strong MFA makes identity verification unnecessary.

- **Reality:** MFA and identity verification answer different questions. MFA helps establish whether someone controls the required authenticators; identity verification helps establish whether the individual corresponds to the claimed real-world identity. Neither independently addresses all identity risks throughout the lifecycle.
- **Leadership action:** Use authentication and identity verification as complementary controls within a broader identity threat detection strategy. Establish identity appropriately, authenticate securely, and continue evaluating identity risk after access has been granted.

Myth 9: Account recovery is a customer service or help desk process, not an identity security event.

- **Reality:** Account recovery and credential reset are among the highest-risk identity events because they can effectively transfer control of an account from a legitimate user to an attacker. Threat actors increasingly target help desks and customer support processes precisely because these workflows can circumvent otherwise-strong authentication controls.
- **Leadership action:** Treat recovery and reset workflows as high-risk identity events. Integrate identity threat detection and risk-based verification into help desk and customer service processes, applying stronger controls when signals indicate elevated risk. High-profile incidents such as the [MGM compromise](#) demonstrate the potential consequences when social engineering succeeds against support processes.

Customer experience and privacy misconceptions

Myth 10: More verification friction automatically means better security.

- **Reality:** Adding friction indiscriminately can reduce completion rates, increase support costs, frustrate legitimate users, and encourage workarounds without necessarily stopping sophisticated attackers. More friction does not automatically equal more security.
- **Leadership action:** Apply friction based on risk rather than applying it equally across all interactions. Use identity threat detection to identify higher-risk interactions and dynamically introduce additional verification or authentication controls where they provide meaningful security value.

Myth 11: Low friction means weak security.

- **Reality:** Strong identity security does not require every legitimate user to undergo the same intrusive process. Low-risk interactions can often proceed with minimal friction when sufficient signals support the trust decision, while higher-risk activities can trigger stronger controls.
- **Leadership action:** Use adaptive, risk-based controls to apply the appropriate level of friction throughout the identity journey. The objective is to make defensible, proportionate, and continuously informed trust decisions—not to maximize friction.

Myth 12: Collecting more personal data always improves identity security.

- **Reality:** Additional data can strengthen certain identity decisions, but indiscriminate collection also increases privacy, retention, consent, regulatory, and customer-trust risks. More data does not inherently produce better identity decisions.
- **Leadership action:** Collect and retain only the data necessary to make effective risk decisions. Evaluate identity security solutions based not only on detection capabilities but also on privacy, data minimization, residency, retention, and regulatory requirements.

Architecture and strategy misconceptions

Myth 13: HR or CRM is already the source of truth, so additional identity controls are redundant.

- **Reality:** A system of record like a CRM or HR system reflects what an organization believes about an identity; it does not necessarily prove that the underlying identity

This Omdia White Paper was commissioned by ID Dataweb and is distributed under license from TechTarget, Inc.

remains trustworthy. Fraudulent employees, compromised customer accounts, stale records, account takeover, and unauthorized changes can all exist while HR or CRM records appear legitimate.

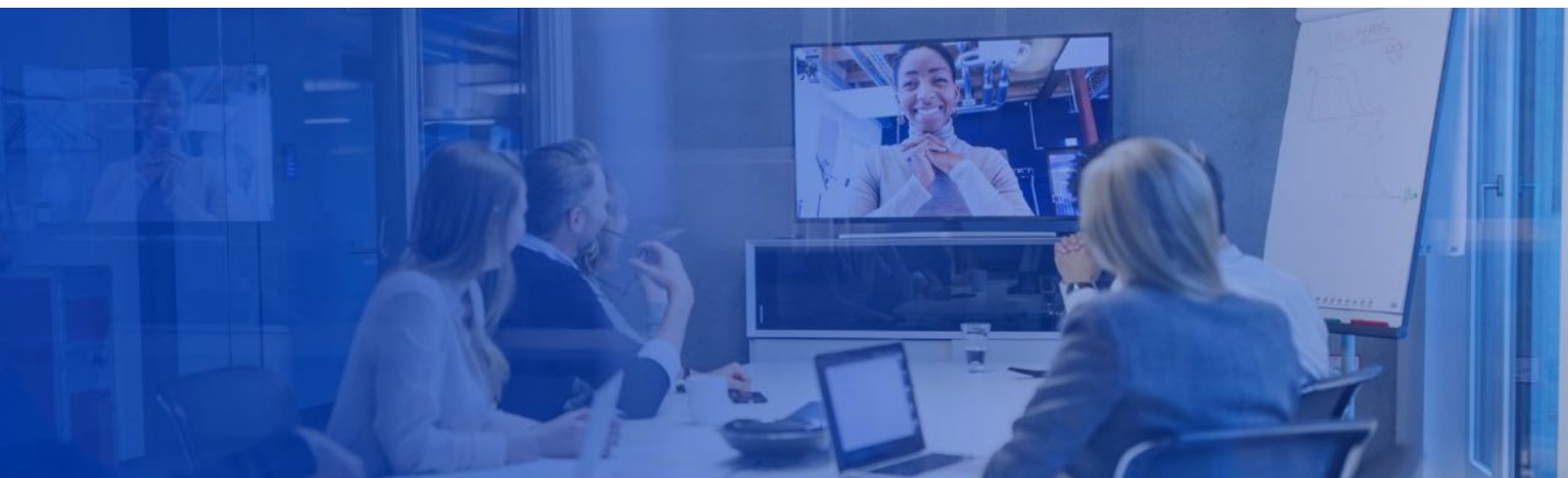
- **Leadership action:** Do not equate a system of record with a source of identity trust. Apply appropriate verification and identity threat detection controls throughout the lifecycle, particularly when identities are created, recovered, modified, granted additional privileges, or associated with high-risk activity.

Myth 14: Identity security performance stays reliable once the program is deployed.

- **Reality:** Identity threats continually evolve. Attack techniques, AI capabilities, user behaviors, devices, document types, regulations, data sources, and organizational processes change over time. Controls that perform effectively today may become less effective as adversaries adapt.
- **Leadership action:** Treat identity security as a continuously evolving program rather than a one-time deployment. Measure outcomes, monitor emerging threats, test controls, tune risk models and policies, and regularly reassess whether identity threat detection capabilities remain effective.

Myth 15: AI agents are primarily an application or data security issue.

- **Reality:** AI agents introduce a new identity security challenge. AI agents can act autonomously or on behalf of humans, access applications and sensitive data, invoke APIs, interact with other AI agents, and execute actions using delegated privileges. And, unlike their human counterparts, AI agents have no ethics and do not worry about being fired. As their autonomy increases, organizations must understand not only what an AI agent is but also who authorized it, whose authority it is exercising, what it is permitted to do, and whether its behavior remains consistent with its intended goal.
- **Leadership action:** Treat AI agents as identities that require visibility, authentication, authorization, governance, and continuous threat detection. Establish clear ownership, apply least-privilege and fine-grained access controls, monitor AI agent behavior and delegated authority, and detect anomalous activity throughout the AI agent lifecycle. Identity and security teams should become involved early in AI initiatives so appropriate controls are designed into deployments rather than added after the fact.



Continuous identity threat detection delivers better outcomes

Enterprises do not need to verify every identity in the same way at every touchpoint. Instead, they need to make defensible, proportionate, and continuously informed trust decisions based on the risk associated with the identity, context, and action being performed.

The goal is not maximum friction or absolute certainty—something that could bring a business to a grinding halt. The right goal is achieving the right level of identity confidence for the right individual, at the right time, and in the right context. Achieving this balance requires organizations to protect against identity-based attacks while preserving privacy, workforce productivity, customer experience, and business growth.

This requires moving beyond point-in-time identity verification toward **continuous identity threat detection**. By combining identity verification with credential, device, behavioral, and other risk intelligence, organizations can identify changes in identity risk throughout the lifecycle and apply additional controls when and where they are needed.

Understanding identity threats, common misconceptions, and potential control gaps enables organizations to strengthen existing identity security programs and adopt a more mature approach—one that continuously evaluates trust, detects emerging threats, and responds appropriately as risk change.

Appendix

Methodology

This White Paper is based on an in-depth review of the market that includes the following:

- Analysis using Omdia's market forecasting data and Enterprise Strategy Group (now Omdia) end-user survey data.
- Vendor interviews that include briefings on current solutions and future plans.

Further reading

- [Fundamentals of Identity Verification](#) (June 2025).
- Complete Survey Results: [Identity Security at a Crossroads: Balancing Stability, Agility, and Security](#) (October 2025).
- Complete Survey Results: [AI Agents and Identity Security: How Enterprises Are Rewriting the Rules](#) (May 2026).

Todd Thiemann, Principal Analyst, Cybersecurity (Identity Security, Data Security, Data Protection)

askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B Materials information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com



Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.