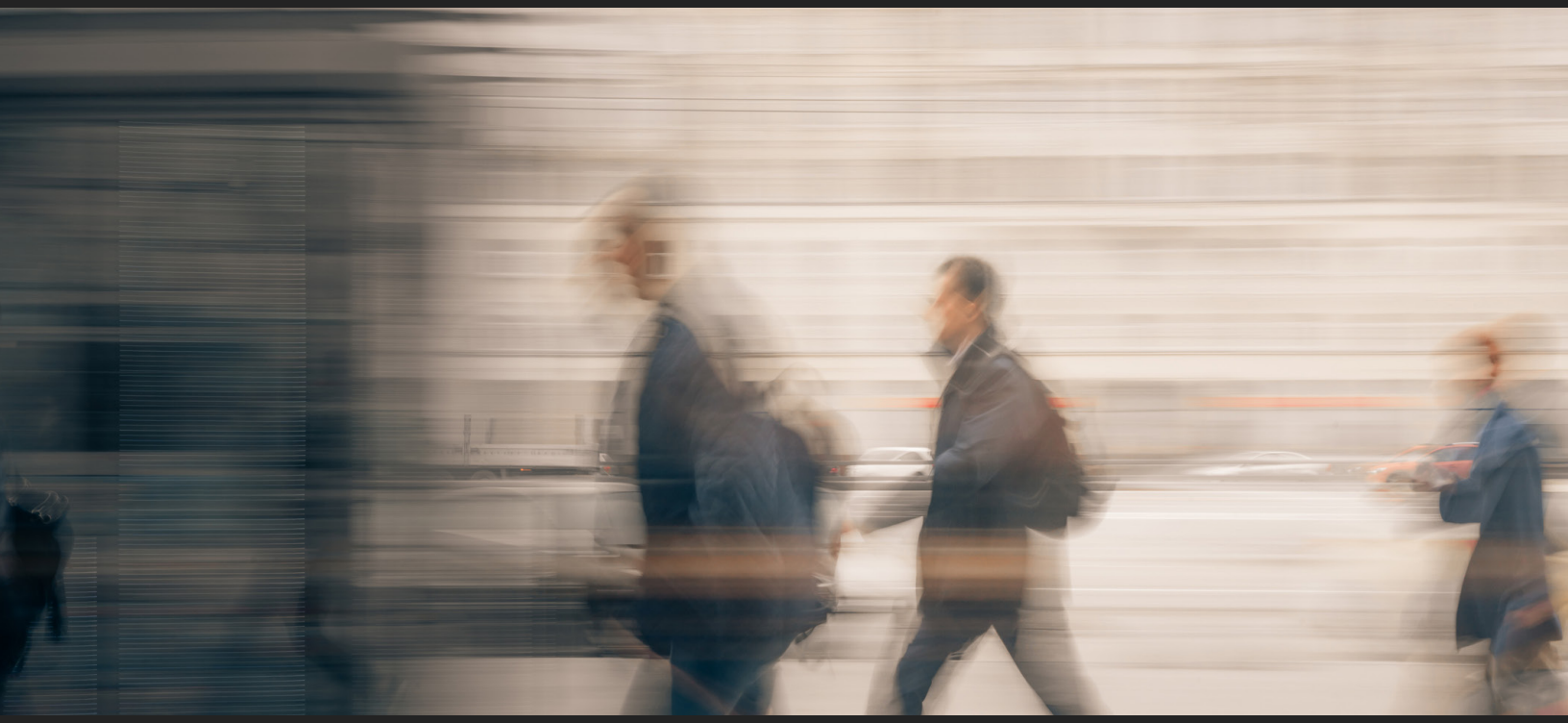

Account Takeover Prevention for Email Providers, MDR, and Identity Risk Teams

Proactively defend customer accounts and workforce identities against credential-based fraud.

Account Takeovers (ATOs) are the primary vector for modern financial fraud and data breaches, often executed using stolen credentials harvested by infostealer malware weeks before traditional defenses react.

Constella's ATO Prevention API empowers platform providers and identity risk teams to detect and respond to credential compromises in real-time. By integrating the world's largest breach data lake directly into your authentication and fraud workflows, you can stop attackers at the front door.

Key Challenges

The Credential Crisis
Infostealers have industrialized the theft of login data, bypassing MFA and static rules.

Latency Kills
Traditional threat intel feeds are too slow for real-time fraud decisions during login or transaction authorization.

Identity IS the Perimeter
For banks and telcos, the customer identity is the new firewall. Protecting it requires visibility beyond your own logs.

How It Works

1 Real-Time Exposure Detection

Query the API with an email, phone number, or username to instantly validate identity integrity against:

- Real-time Breach Feeds
- Active Infostealer Logs
- Underground Market Listings

2 Structured Identity Risk Signals

Receive actionable JSON insights in milliseconds:

- Exposure Source & Timeline: Know when and where the data was stolen.
- Malware Context: Identify if the user is infected with active malware (RedLine, Raccoon, etc.).
- Password Hygiene: Detect use of known weak or previously compromised passwords.

3 Automated Risk Response

Integrate with SIEM, SOAR, CIAM, or Fraud Decisioning engines to:

- Force Password Resets: Automatically trigger remediation for compromised users.
- Step-Up Auth: Trigger MFA or biometric checks for high-risk logins.
- Block Transactions: Prevent fraudulent transfers from compromised accounts.

Why Constella

Infostealer Intelligence:
Deep coverage of stealer logs and active threat actor tactics.

Ultra-Fast Response:
Sub-second lookup speeds (<200ms) for seamless user experiences.

Global, Verified Data:
1 Trillion+ attributes across 125+ countries and 50+ languages.

Built for Scale:
API-first architecture handling millions of daily requests.

Key Benefits

Prevent Fraud Before Login: Stop account takeovers at the perimeter by detecting exposed credentials before attackers act.

Accelerate Response with Automation: Deliver near real-time decisions via API—no manual review needed

Enhance Fraud Models: Enrich existing workflows with high-fidelity identity signals that go beyond behavioral or device telemetry.

Built for High-Stakes Identity Protection

- Email and cloud service providers
- MDR and XDR providers
- Identity Threat Detection & Response (ITDR) teams
- IAM and CIAM providers
- Fraud and risk operations
- Financial services and fintech organizations

Integrate credential exposure intelligence into your detection and response workflows today.

Let's connect. Visit Constella.ai to learn more.

Constella

Constella Intelligence is a global leader in identity risk intelligence, helping organizations detect, investigate, and respond to threats linked to exposed personal data. Powered by the world's largest breach and infostealer data lake, spanning over one trillion attributes across 125+ countries and 50+ languages, Constella delivers unmatched visibility into identity threats across the surface, deep, and dark web. Enterprises and technology partners worldwide rely on Constella to strengthen identity posture, fuel threat intelligence, and reduce digital risk. Learn more at constella.ai.

javelin DARK WEB THREAT INTEL VENDOR SCORECARD BEST IN CLASS 2025

2025 SINET16 INNOVATOR AWARD