Identity Intelligence

Intelligence-Driven Identity Fraud Prevention

Challenge

Strong identity authentication is more important than ever before as organizations face an expanding threat landscape and unprecedented level of attacks. Dynamic ecosystems of employees, customers, and partners are facing the sharp increase in account takeovers by adversaries, looking to steal credentials so they can access and initiate fraudulent activities.

This is further compounded by the rapid growth in remote work and digital interactions across multiple channels, which provides new challenges for security and IT teams responsible for securing the identities of employees, customers, and third parties.

Solution

The Recorded Future Identity Intelligence module enables security and IT teams to detect identity compromises for both employees and customers, and respond confidently — without any manual research. Recorded Future automates the collection, analysis, and production of intelligence from a vast range of open source, dark web, and technical sources, and combines it with world-class research to help drive an accelerated response by your security team. This approach produces real-time intelligence at massive scale, offering an unmatched source of truth for identity authenticity.

Identity Intelligence enables users to monitor for identity compromises in real time, and access critical details, such as password length, complexity, and whether the leak was novel or recycled. Armed with this real-time evidence, security and IT teams are able to quickly prioritize identity threats and initiate downstream response workflows, integrated directly into their existing security and identity tools. By automating information aggregation and triage, the module significantly reduces the time needed to address identity fraud and business risks.

Benefits

- Detect stolen credentials in real time through automated monitoring of criminal forums and malware logs so you can quickly take action before attackers can exploit them.

- Prevent unauthorized access before breaches occur by detecting compromised customer credentials across dark web sources and automating workflows into your existing authentication systems.

- Instantly mitigate threats by automating password resets, MFA enforcement, risk checks, and access restrictions through direct integration with your IAM and SOAR platforms.

Use Cases

- Monitor for identity compromises across open, dark web, and technical sources.

- Detect credential leaks in real-time before business impact occurs.

- Prioritize identity threats based on password complexity and leak novelty.

- Provide evidence for updating or resetting compromised identities.

- Analyze identity threats with insights into related domains and technologies.

- Initiate automated response workflows when compromised credentials are detected.

53%
of teams that now have a significantly better understanding of their organization's digital footprint by using Recorded Future

34%
average time users reduced on digital footprint analysis

Results

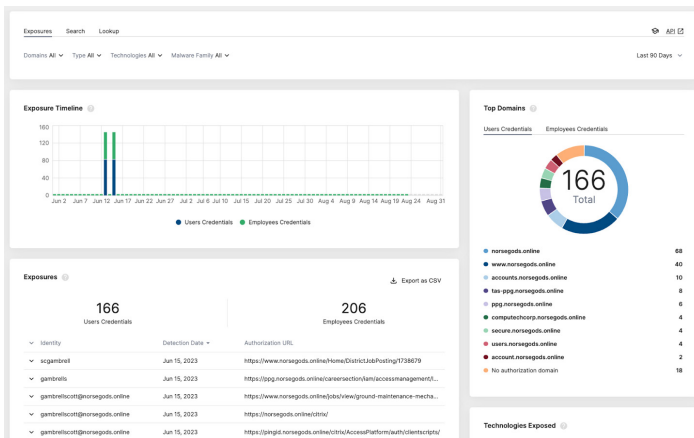|	
Real-time credential leak detection in one view	Identify, analyze, prioritize, and respond to identity compromises with insights into related domains, technologies, and infostealer malware in Identity Home.
Comprehensive credential lookup	Search for exposed credentials by entering specific identifiers (e.g., email, username, password, or hash) and view comprehensive details including detection dates, authorization URL, and malware source information.
Advanced querying	Identify exposures within your approved domains by filtering via password requirements, domain types, malware family, and download dates.
Comprehensive sourcing	Access identity exposure data in real time across open, dark web, and technical sources—including infostealer malware logs that other security solutions can't access.
Prioritized alerts	Easily prioritize credential breaches thanks to automatic categorization of exposure alerts as high priority (high-risk credentials), medium priority (info stealer malware), or low priority (public leaks/database dumps).
Full breach analysis	Examine all credentials (70 per host on average) stolen from a compromised machine with Incident Reports.
Expert security intelligence team access	Access to a team of world-class security intelligence experts for onboarding, training, and ongoing support
Expert security intelligence team access	Access detailed analysis and context on major infostealer security incidents from Insikt Group, Recorded Future's threat research team.

See Identity Intelligence in action

[Request a demo](#) to learn how you can make fast, effective, data-driven decisions with Recorded Future.

"The timeliness is a big win with Identity Intelligence. Being able to automate the response after seeing an alert to our active directory allows us to feel confident that the account is secure."

Curtis Hartsell
Senior Cyber Threat Intelligence Manager, Toyota Motors North America **(See the case study)**

"Thanks to the Recorded Future Managed Services team we caught on to our internal user's credentials leaking before anything could happen, and that helped us to prevent significant damage."

Security Analyst
Security Analyst, Medium-sized enterprise internet software and services company **(UserEvidence)**