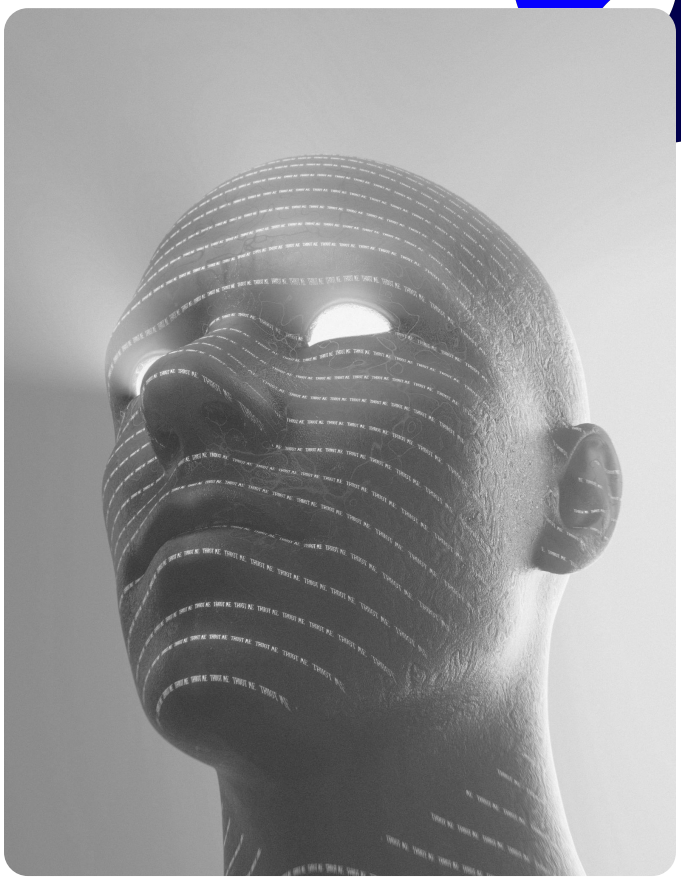
Recorded Future®

EXECUTIVE INSIGHTS REPORT | OCT 2025

Synthetic Identities
A Dual Threat to Enterprises

From Insikt Group®



Summary

Synthetic identities — digital personas crafted from real and fabricated data — represent a dual threat to enterprises, **enabling large-scale financial fraud**, while also facilitating **state-sponsored sanctions evasion, illicit revenue generation, and intellectual property (IP) theft.**

Advances in generative AI (GenAI) and deepfake technology mean **adversaries can create highly convincing synthetic personas** which, when combined with social engineering and injection-based techniques, can evade know-your-customer (KYC) checks and biometric liveness detection.

To withstand this threat, organizations must adopt a more rigorous approach to identity verification and remote work security, ensuring that **every identity, interaction, and transaction is continuously validated.**

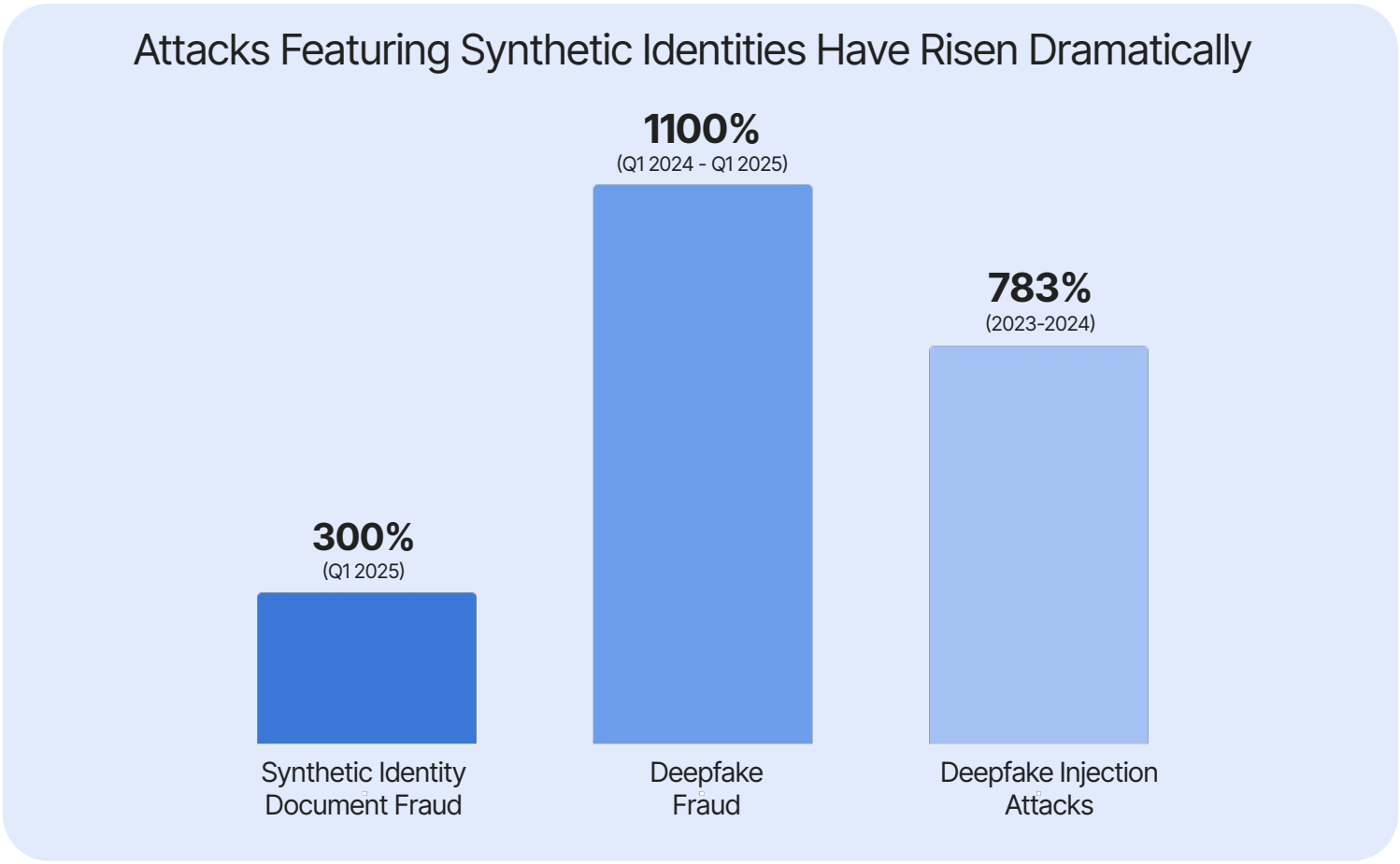


Figure 1: *Synthetic Identities: Key Statistics (Source: Recorded Future)*

Synthetic Identities: A Dual Threat

Synthetic identity fraud (SIF) is one of the fastest-growing categories of financial crime. It involves creating a fake identity by combining legitimate information (for example, stolen Social Security numbers or driver's license data) with fabricated information (such as made-up names, dates of birth, or addresses). The result is an identity that appears real on paper but does not represent an actual person.

Criminals typically build up synthetic personas over time, opening bank accounts and establishing credit histories until they can secure large loans. Because no real victim exists to raise an alarm, and some components of the identity are legitimate, traditional fraud detection methods often fail to recognize SIF. Once the funds are obtained, the criminals can disappear, leaving financial institutions to absorb the losses.

Beyond financial fraud, synthetic identities have also evolved into a vehicle for insider threats. Adversaries are increasingly using them to enter organizations as remote employees or contractors, gaining legitimate digital credentials and access privileges. This is particularly dangerous because there is no real individual behind the profile to monitor, yet they operate with the same trust as genuine insiders.

Generative AI: A Force Multiplier

SIF is accelerating at an unprecedented pace. In Q1 2025 alone, synthetic identity document fraud rose by 300%, while deepfake-enabled fraud has increased more than tenfold since the start of 2024. This escalation is fueled by the widespread availability of free, easy-to-use AI tools and services, which enable even unskilled criminals to generate convincing passports, ID documents, and even synthetic biometric data such as facial images, fingerprints, and iris patterns.

The most alarming development is the rise in deepfake injection attacks, which in 2024, spiked by 783% from 2023. Unlike traditional presentation attacks that replay manipulated media on a screen, injection attacks feed synthetic media directly into the verification pipeline. This makes it appear as if data is captured live by the user's device, enabling adversaries to animate synthetic identities in real time. These techniques have already proven successful at breaching KYC safeguards and infiltrating organizations through remote hiring channels.

Case Study: North Korean IT Employment Scam



Figure 2: *Original Photo (Left) And AI Fake (Right) Used By A North Korean Threat Actor Who Posed As A Us-Based Software Engineer And Was Hired By Cybersecurity Firm Knowbe4 (Source: Knowbe4)*

The most striking example of synthetic identity abuse is North Korea's IT employment scheme, which Insikt Group tracks as PurpleDelta. While not every case involves fully synthetic identities, many operators have combined stolen personal identifiers or identities "loaned" by paid facilitators, with fabricated profiles across LinkedIn, GitHub, and other social media and job boards, to secure remote jobs or contractor roles at US firms. Evidence also indicates the use of deepfake injection techniques to pass remote hiring processes. Once hired, they often work through "laptop farms" — clusters of devices run by accomplices configured to mimic local employees and blend seamlessly into enterprise networks.

This scheme has proven highly effective, with confirmed infiltrations affecting at least 64 US companies and numerous reports indicating the true number may be significantly higher. Targets have included leading technology firms such as SentinelOne and Google, US government contractors including NASA's Jet Propulsion Lab, and multiple Fortune 500 enterprises. Each worker is estimated to generate up to $300,000 annually, funneling millions to the North Korean regime while also providing potential access to intellectual property, sensitive data, and persistent footholds across global IT supply chains.

Why Detection is Failing

Despite increased awareness around synthetic identities, both technological and human defenses remain inadequate. Independent testing shows that many identity verification platforms overstate their ability to detect deepfakes, particularly injection attacks. This gap between marketed capabilities and real protection exposes organizations to risk while fostering a false sense of security. The problem is compounded by knowledge gaps: The 2025 RSA ID IQ5 Report revealed that nearly half of respondents failed basic identity security questions, with identity and access management (IAM) and cybersecurity professionals performing worst of all.

Human detection is equally unreliable. A 2025 study revealed that only 0.1% of participants could correctly identify all synthetic media, with fewer than one in ten recognizing deepfake videos. One-third of adults over 55 had never heard of deepfakes, while younger adults (18–34) showed misplaced confidence despite poor detection rates. Even when individuals correctly identify synthetic media, awareness and reporting rates remain low across enterprises, with 29% of employees admitting they would take no action at all. Together, these weaknesses reveal a society and workforce unprepared for the growing threat of synthetic identities.

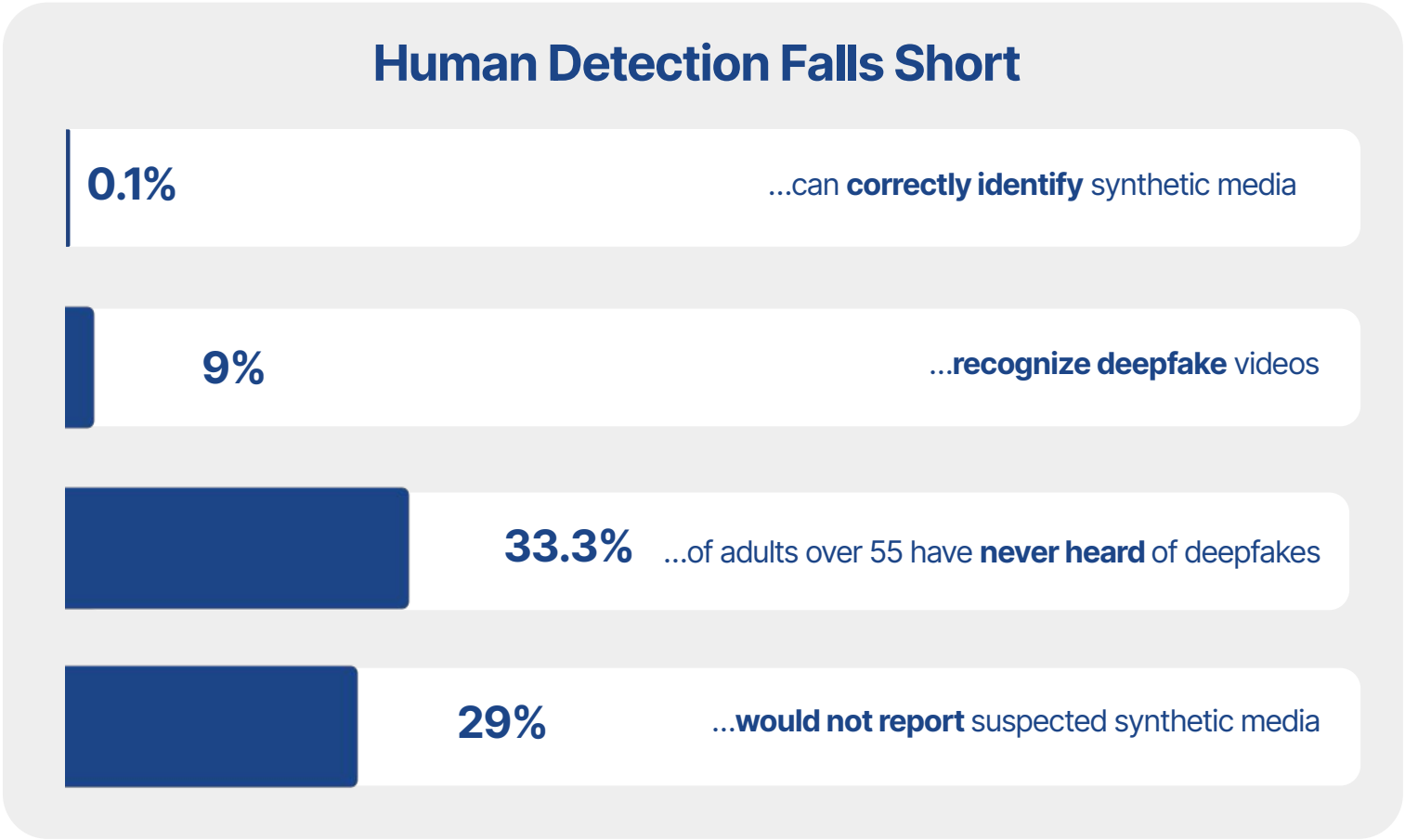


Figure 3: *Human Deepfake Detection Statistics (Source: iProov)*

Risks for Enterprise: Sanctions, Spies, and Stolen IP

The rise of synthetic identities underscores a shift in adversary behaviour from targeting individual consumers to exploiting enterprises. Threat actors are increasingly abusing remote hiring, digital identity verification, and executive communications to achieve higher-value payouts. This evolution carries severe financial consequences: Across the US, identity-related crimes cost businesses $8.8 billion in 2022, with an average loss of $4.24 million per incident. Projections suggest that SIF alone could drive annual losses of $58.3 billion by 2030.

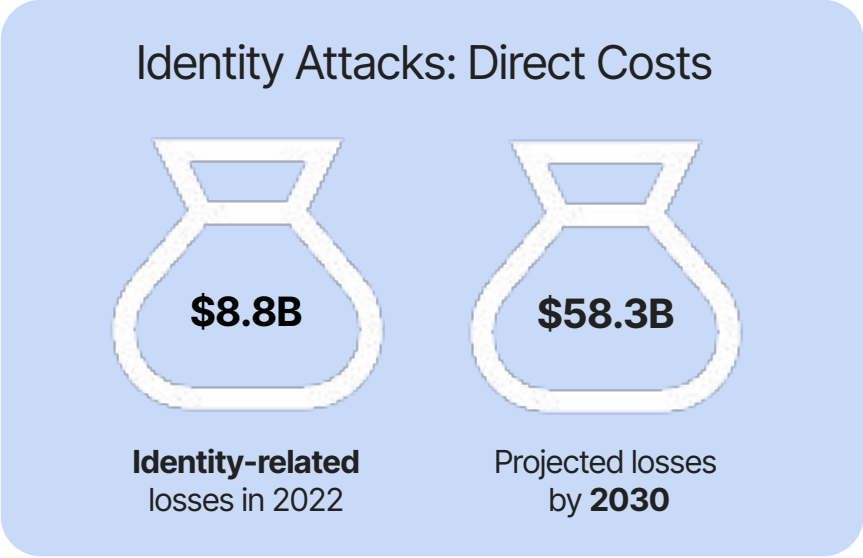


Figure 4: *Direct Costs of Identity Attacks (Source: FTC; Juniper)*

Beyond immediate financial loss, employing sanctioned individuals, even unknowingly, exposes organizations to regulatory fines of up to $377,700 per violation or twice the value of the transaction (whichever is greater), as well as criminal penalties of up to $1 million and twenty years' imprisonment for willful breaches. For example, if a company paid a disguised North Korean IT worker $500,000 in wages, the civil penalty alone could reach $1 million, with far greater consequences if the violation were deemed egregious.



Figure 5: *Hidden Costs of Synthetic Identity Attacks (Source: Recorded Future)*

Employing malicious operatives also presents a critical risk to organizations' IP and internal security. Operators exploiting fake or stolen identities have infiltrated US companies, with at least one being a California defense contractor, and siphoned confidential technical data and virtual currency. Such breaches erode competitive advantage, especially in high-value sectors like defense and advanced technology. Increasingly, these incidents are now extending into extortion, with threat actors stealing sensitive information and demanding payment to avoid public exposure.

Outlook

Distinguishing between real and synthetic humans will likely become a core challenge for businesses and governments. Fraudsters will continue to create digital personas blending stolen personally identifiable information (PII), AI-generated data, and fabricated activity histories. With deepfake-enabled video and voice, these identities will not only exist on paper, they will "show up" in onboarding calls, customer service interactions, and social media networks.

State-sponsored infiltration via synthetic hiring will likely expand. Other adversarial states, such as China and Iran, could seek to replicate North Korea's playbook as a low-cost, high-reward strategy for sanctions evasion, espionage, and financial gain. This will make insider risk and supply chain integrity critical national security issues.

Governments will almost certainly tighten identity verification and sanctions compliance requirements. Identity verification standards will almost certainly become procurement-critical in regulated private sector industries such as finance, defense, and technology, with companies facing more rigorous audits, mandatory adoption of advanced screening tools, and increased liability for failing to detect synthetic identities.

Identity management will likely evolve into a zero-trust model, where every interaction is actively validated. Static verification methods (passwords, ID scans, one-time biometrics) will likely become obsolete. Enterprises will be forced to adopt continuous, multi-layered trust models that include behavioral biometrics, device trust signals, cryptographic watermarking of media, and secondary verification channels.

Further Reading

SOURCE	TITLE
Insikt Group	Inside The Scam: North Korea's IT Worker Threat
Insikt Group	Annual Payment Fraud Intelligence Report: 2024
iProov	Threat Intelligence Report 2025 Remote Identity Under Attack

Mitigations

Secure Identity with AI: While AI amplifies the risks associated with synthetic identities, it can also be part of the solution. Organizations should deploy AI-powered detection platforms capable of identifying injection-based attacks, manipulated biometrics, and fraudulent credential trails in real time. Continuous anomaly monitoring of employee behavior and access patterns should complement identity screening. Extend this to detect unauthorized use of remote access or remote monitoring tools (such as AnyDesk and TeamViewer), which may indicate laptop farm connections or misrepresented work locations. Recorded Future's Identity Intelligence can help to detect compromised credentials that may be used in SIF.

Govern Remote Hiring and Access: Refuse to provision hardware or network access until in-person or notarized identity validation is complete, particularly for high-risk roles. Incorporate multi-factor biometric authentication and liveness checks into hiring and onboarding. Escalate suspicious resumes or hiring signals early, treating talent acquisition as part of the security perimeter. Align practices with MITRE D3FEND techniques such as *Process Access Pattern Analysis (D3-PAPA)* and *Remote Access Detection (D3-RAD)* to harden against covert access attempts.

Integrate Threat Intelligence into Identity Workflows: Use Recorded Future's Threat Intelligence to track fraudulent digital identities, laptop farms, and infiltration schemes linked to state-backed adversaries. Feed this intelligence into HR, compliance, and SecOps workflows.

Align with Regulations: Map digital identity processes against emerging frameworks such as the EU Digital Identity Regulation and US sanctions compliance obligations. Prepare for procurement requirements where identity verification and sanctions attestation are mandatory.

Transition to Continuous, Zero-Trust Identity Models: Move beyond static verification to continuous, multi-layered trust models. Combine behavioral biometrics, device trust scoring, cryptographic watermarking of media, and secondary verification channels. Adopt a "never trust, always verify" approach across all high-value digital interactions.

Risk Scenario

Scenario: A Fortune 500 technology company unknowingly hires a synthetic persona linked to a North Korean operator. Over time, the operative gains elevated access, siphons proprietary IP, and compromises supply chains.



First-order Implications

Threat

Privileged insider access enables the threat actor to exfiltrate trade secrets and customer data.

Injection-based deepfakes bypass verification controls during ongoing identity checks.

Risk

Financial: Direct regulatory fines for sanctions violations, incident response costs, and revenue loss from disrupted contracts.

Operational: Service outages and compromised research and development (R&D) pipelines.

Compliance: Mandatory breach disclosures and sanctions-related penalties.



Second-order Implications

Threat

Threat actors pivot through compromised accounts into partner ecosystems, extending exposure across suppliers and subcontractors.

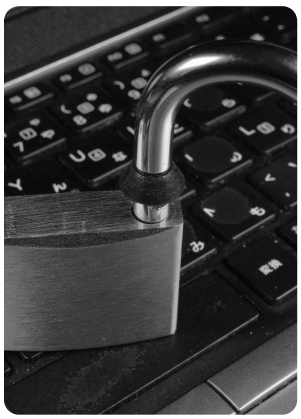
Regulators initiate probes into corporate hiring and identity verification practices.

Risk

Brand: Public exposure erodes external trust (with business partners and regulators, for example) in hiring processes and enterprise governance.

Financial: Extended remediation timelines result in contract losses and insurance premium hikes.

Legal: Class-action lawsuits emerge from claims of negligent identity vetting.



Third-order Implications

Threat

State-linked adversaries use infiltrations to seed destructive follow-on attacks, disguised as insider negligence.

Intellectual property exfiltration fuels competitor products and adversarial state programs.

Risk

Geopolitical: Attribution to North Korea escalates sanctions and retaliatory measures, straining global operations.

Competitive: Loss of innovation advantage.

Systemic: Sector-wide regulatory overhaul enforces stricter hiring and identity standards, raising costs for all firms.

Key

Legal or compliance failure: Breach of laws, regulations, or industry standards resulting in liability or sanctions.
Operational disruption: Interruption to normal business processes affecting productivity or service delivery.
Brand impairment: Damage to reputation that reduces customer trust and market value.
Financial fraud: Unauthorized manipulation or theft of financial assets for personal or organizational gain.
Competitive disadvantage: Loss of market position due to inferior capabilities, intelligence, or innovation.

References:

The Risk Business: Second Edition
Intelligence to Risk
The Intelligence Handbook

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform delivers end-to-end visibility across adversaries, infrastructure, and targets. Powered by precise AI-driven analytics and the proprietary Intelligence Graph®, the platform enables organizations to see the complete picture, act with confidence, and get ahead of threats that matter. With real-time intelligence built from over 15 years of threat data, Recorded Future supports security teams in proactively defending against evolving threats. Headquartered in Boston with global offices, Recorded Future works with over 1,900 businesses and government organizations across 80 countries. Learn more at www.recordedfuture.com.

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.