1,000,000,000
IDENTITY RECORDS EXPOSED

At A Glance

Customer: Global Technology & Semiconductor Innovator (Fortune 500)

Industry: Technology / Manufacturing

Challenge: Targeted executive impersonation (Deepfakes) and doxxing of leadership during a high-stakes merger.

Solution: Constella Hunter+ (DRPS)

Outcome: 100% of malicious domains removed, physical security threats neutralized, and a $5M+ fraud attempt prevented.

> *"We were blind to the threats incubating outside our network. By the time an impersonation email hit our gateway, the damage was already done. We needed to see the attack forming in the wild."*
>
> Chief Information Security Officer (CISO)

Defending the C Suite

How a Fortune 500 Tech Leader Stopped a Multi-million Impersonation Attack.

THE CHALLENGE: Innovation Brings Targeted Risk

As a global leader in semiconductor technology, Constella's customer operates at the intersection of high-value intellectual property and geopolitical sensitivity. Following the announcement of a strategic acquisition, the company's attack surface exploded.

The CISO identified three critical threat vectors that traditional security tools (Firewalls, EDR) could not see:

1. **Executive Doxxing:** The CEO's home address and family details were circulated on Telegram channels and dark web forums, escalating physical security concerns.
2. **Synthetic Impersonation:** Threat actors created convincing "deepfake" audio clips of the CFO to authorize fraudulent wire transfers.
3. **Brand Erosion:** A network of typo-squatted domains emerged, hosting fake press releases designed to manipulate the company's stock price.

THE SOLUTION: Constella Hunter+, Visibility Beyond the Perimeter

The client deployed Constella Hunter+, a managed Digital Risk Protection Service (DRPS), to establish a protective dome around their brand, assets, and key executives.

By leveraging Constella's data lake of over 1 Trillion recaptured assets, the solution provided:

- **Continuous Digital Footprint Monitoring:** Real-time scanning of the Surface, Deep, and Dark Web for mentions of 50+ Key Executives (VIPs).
- **Infostealer Intelligence:** Automated detection of compromised credentials belonging to the workforce and executive family members.
- **Adversarial Takedowns:** Rapid remediation of malicious domains and social media impersonations.

Constella

THE INCIDENT: Stopping the Attack Before Execution

Three weeks into deployment, Constella's Fusion Center analysts detected a critical signal: a "Kit" for impersonating the client's CFO was being sold on a closed Russian-language cybercrime forum. The kit included:

- Stolen credentials for the CFO's personal email (harvested from a third-party breach).
- AI-generated voice memos mimicking the CFO.
- A list of the company's accounts payable vendors.

The Constella Response:

- **Detection (Hour 0):** Constella's AI correlated the stolen credentials with the forum listing, generating a Critical Severity Alert.
- **Validation (Hour 1):** Human analysts confirmed the authenticity of the threat and identified the threat actor's infrastructure.
- **Remediation (Hour 4):**
    - The client's security team forced a global password reset for the affected executive.
    - Constella initiated takedowns for the hosting infrastructure storing the deepfake assets.
    - Law enforcement was notified with an attribution package identifying the actor's location.

THE RESULTS: Reputation Saved, Fraud Prevented

By shifting from reactive defense to proactive intelligence, the client achieved:

- $5 Million+ Saved: Prevention of a verified BEC (Business Email Compromise) wire fraud attempt.
- 95% Reduction in Response Time: Moving from weeks of manual investigation to same-day remediation.
- Executive Peace of Mind: The physical security team now receives automated alerts regarding travel risks and location exposure for traveling VIPs.

CUSTOMER IMPACT

> *"Constella didn't just give us data. They gave us time. They found the needle in the haystack, the one credential that would have opened the door to our entire treasury, and helped us close the lock before the attackers arrived."*
>
> VP of Global Security Operations

Partner with Constella to extend your detection capabilities, reduce identity risk, and stay ahead of emerging threats.

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