Illusive Networks for Banking and Financial Services

Early detection and on-demand forensic intelligence to stop high-impact, sideways attacks

Financial institutions are one of the most high-value targets for cyberattackers who "follow the money" and those intent on systemic disruption. Despite the vast resources financial institutions devote to cybersecurity, one challenge has been especially difficult to solve: the challenge to detect and stop APTs and malicious insiders before real damage is done. It is inherently difficult to identify attackers who move through the network with valid credentials and sophisticated tools to cover their tracks—but complex ecosystems, continuous business innovation, M&A activity, cloud adoption, fintech, and a growing consumer-driven attack surface multiply the problem for financial entities—and increase the importance of early attack detection.

Security operations teams, though outfitted with dozens of advanced technologies, are besieged by alerts. High-impact incidents can remain well-camouflaged for months and go undetected until the damage has been done.

Reversing the risk equation

Illusive plants featherweight deceptions on every endpoint to mimic the real data, credentials, and connections the attacker needs. Confronted with a distorted view of reality, the attacker is overcome by the odds: it is impossible to choose a real path forward without activating a deception.

Unknown to the attacker, one wrong choice triggers a notification to the security team. Incident responders can see how far the attacker is from critical business assets. With real-time forensics in hand, they can take informed actions to stop the attack and avert business impact.

By focusing on the attacker's process rather than on the tools or malware they're using, organizations are better protected from unknown, evolving threats, and can detect malicious behavior— regardless of what gaps may exist in their security controls. Enabled by intelligent automation, Illusive's approach scales and adapts—so the business can operate with greater confidence.

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.
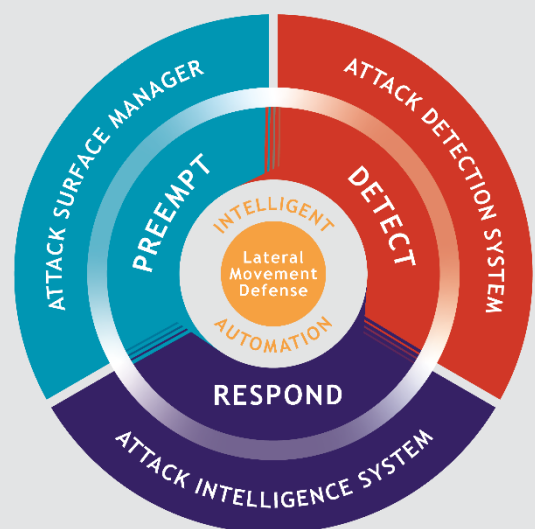
Changing the math for early attack detection

Reducing the number of real artifacts while saturating endpoints with deceptive ones increases the odds that attackers will choose deceptions—and be instantly caught.

The Illusive Platform empowers Banking and Financial Services Organizations to:

- **Reinforce a risk-focused approach.** Whether your concerns are fraud prevention, customer privacy, protection of proprietary algorithms and formulas, or disruption of trading, settlement operations or online banking, Illusive focuses security attention on critical assets. Operators can see attackers' proximity to your crown jewels early in the attack cycle, buying time for a careful response.

- **Protect both old and new.** Mainframes and legacy applications can be difficult to monitor but can be essential to business performance. Monitoring for lateral movements toward them provides a powerful alternative or enhancement to traditional monitoring approaches.

- **Report on and reduce attack risk.** Illusive's dashboard provides rich metrics to quantify APT attack risk, along with the ability to remove errant credentials, connections, and potential attack pathways—helping to provide visibility and assurance to directors and stakeholders.

- **Reduce SOC noise.** Deceptions are transparent to authorized users and visible only to malicious actors so there are zero false positives. Every Illusive notification is reliable and warrants investigation.

- **Deploy distributed deceptions at scale—rapidly and without agents.** Illusive auto-discovers your systems and their connections as an attacker would see your network. Intelligence-driven automation designs smart, authentic deceptions, which can be deployed at scale in a single click.

- **Easily manage an adaptive deception environment.** Illusive's machine intelligence automatically adjusts deceptions as threats and IT environment change—and creates shifting, uncertain terrain for attackers.

- **Extend source and target forensics and APT risk mapping to other SOC tools.** Through integration with Illusive, SIEM and other technologies can initiate on-demand collection of forensic data and leverage the insights provided by Illusive's comprehensive forensics capabilities.

Illusive Use Cases

- ★ Early Detection & Real-Time Forensics of In-Network Attackers
- ★ Insider Threat Defense
- ★ Attack Surface Reduction
- ★ Compliance Support (SWIFT, FFIEC, PCI-DDS)
- ★ Protecting Difficult-to-Secure Mainframe, OT, IoT, and Network Devices
- ★ M&A Security
- ★ Cloud Security
- ★ SOC Efficiency
- ★ Red Team Exercises

"Illusive provides exceptional, innovative coverage for malicious pivoting and lateral movement. It uncovers the in-depth, sophisticated actors who evade other countermeasures and gives us direct visibility into targeted attacks. That's invaluable."

CISO, OakNorth Bank

"Illusive closes the gap between a targeted attack and awareness of an attacker's presence. It allows us to proactively protect our customers, business, and assets. And it makes my job a lot easier."
IT Manager, US-based bank

"Illusive's Forensics-on-demand capabilities decreased our response time by 90%."
Senior Manager - Digital Forensics, Canadian multi-national bank

Visit us: www.illusivenetworks.com

Email us: info@illusivenetworks.com

Call us::   US: +1 844.455.8748
             EMEA / AsiaPac: +972 73.272.4006

Find us: