Illusive Networks

CASE STUDY

OakNorth Bank

Innovative Lender Deploys In-Depth Protection Against Sophisticated Threat Actors

“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.”

Jerry Finley, Chief Information Security Officer

Illusive deceptions increase team efficiency and cover the bases that other solutions don't

OakNorth Bank

OakNorth Bank is one of the most active lenders in the UK. The Bank helps entrepreneurs and rapid-growth businesses achieve their potential with access to fast, transparent, and flexible debt finance solutions. In addition to lending, OakNorth Bank offers a range of savings accounts. By saving with OakNorth Bank, customers not only benefit from competitive interest rates, they also support the UK's ecosystem of startup companies. OakNorth Bank has lent c.£4bn since obtaining its license in September 2015, directly helping with the creation of 10,000 new homes, 13,000 new jobs, and adding several billion pounds to the economy.

OakNorth Bank

CHALLENGE

- Defend customer and employee information and bank assets from compromise
- Detect and thwart sophisticated attackers who evade other security measures
- Effectively defend cloud-based operations across accounts and instances

SOLUTION

Illusive Networks
Attack Detection System

RESULTS

- Gained deep visibility and end-to-end defense across office-based and AWS-based assets
- Increased security team efficiency with high-fidelity alerts and detailed, actionable forensic information

The Challenge

OakNorth Bank supports its savings and lending activities with offices in London, Manchester, Gurgaon, New York City, and Bangalore. As a cloud-first company, its preference is to always invest in next-generation technology for operations and security infrastructure. In May 2016, with the help of Amazon Web Services (AWS), OakNorth became the first bank in the UK to be fully cloud-hosted. OakNorth Bank also uses AWS to deliver a financial technology service that helps lenders make informed decisions through data and automation. Security is always top of mind, which is one of the reasons the company chose AWS, conducts regular penetration testing, and performs advanced attack simulations. To maximize effectiveness of its layered security infrastructure, the company continually trains its employees and reinforces data security best practices.

"My role is to ensure the privacy and security of our data, clients, and employees," said Jerry Finley, Chief Information Security Officer for OakNorth Bank. "Regardless of where they are located, whether their information resides in our office environment or cloud platform, we want to be prepared to detect and disrupt any emerging cyberthreats."

Learn more about OakNorth Bank at www.oaknorth.com

The Challenge (cont'd)

OakNorth Bank especially wanted to add a layer of protection against sophisticated threats that evade other security measures, such as advanced persistent threats, as well as gain insight into attacker tactics and techniques. The new layer needed to be cloud-based for high scalability and flexibility, and it had to defend the company without time-wasting false positive alerts. The security team looked at deception technology and partnered with Illusive and its Attack Detection System to gain real-time verification of anomalies and lateral movement in the network.

"We chose Illusive because we share their approach of focusing on attackers' behavior and perspective," said Finley. "We also value their strong market reputation. Illusive team members are not just knowledgeable, they are passionate about what they do. Illusive's expertise in attacker methodology augments our internal capability to detect novel attacks, while enabling rapid and adaptable coverage in our cloud-based environment. As a fully cloud-based bank, we expect to work with partners who can be agile, and that's exactly what Illusive provides."

> "We chose Illusive because we share their approach of focusing on attackers' behavior and perspective"
>
> Jerry Finley, Chief Information Security Officer, OakNorth Bank

The Solution

The Illusive Networks Attack Detection System is agentless, intelligence-driven technology that creates a dense web of deceptions and effortlessly scales across the infrastructure. Featherweight deceptions on every endpoint look exactly like the company's real data, access credentials, and connections. When an attacker is confronted with deceptions, this deceptive view of reality makes it impossible to choose a real path forward. One wrong step triggers an alert to the company's security team.

"The concept of creating doubt and confusion in an intruder's mind is well thought-out and invaluable," said Finley. "When attackers can't distinguish between real and deceptive assets, we can collect information and apply intelligence to patterns that we've observed during that time period of activity. With Illusive we simultaneously sharpen our investigative process and constrain the attacker."

OakNorth Bank easily deployed Illusive across its complex environment, scaling it across AWS instances and accounts. Finley and his team now have continuous visibility and confidence that the Illusive defenses enable them to thwart sophisticated threat actors.

Proactive and Efficient

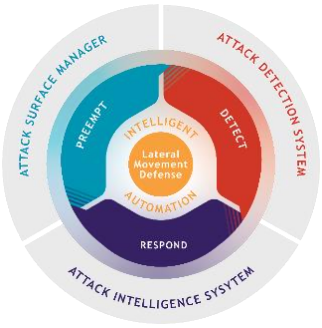
The OakNorth Bank team gained proactive threat response and the assurance that an alert represents a real issue. Illusive alerts are only triggered when an attacker engages with a deceptive asset. At that point, Illusive immediately begins capturing forensic data from the system where the attacker is operating, presenting real-time forensics and a quantifiable measure of potential business risk. For example, Illusive uncovered malicious processes trying to operate on an endpoint.

"Illusive enables us to be much more proactive," said Finley. "It detects and analyzes attacks in real time to produce actionable alerts, directing our team to relevant and valuable conclusions."

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

The Illusive Platform

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.



Preempt: Finds and removes errant credentials, connections, and attack pathways to deter unauthorized lateral movement.

Detect: Forces attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making.

Respond: Enables rapid, effective response and remediation when attackers are present by providing contextual source and target forensics.

For more information

Visit us at www.illusivenetworks.com

Email us at info@illusivenetworks.com

Call us at +1 844.455.8748 (North America)
or +972 73.272.4006 (EMEA and AsiaPac)

Illusive Networks stops cyberattacks by destroying attackers' ability to make safe decisions as they attempt to move toward their targets. Using Illusive, organizations eliminate high-risk pathways to critical systems, detect attackers early in the attack process, and capture real-time forensics that focus and accelerate incident response and improve resilience. Through simple, agentless technology, Illusive provides nimble, easy-to-use solutions that enable organizations to continuously improve their cyber risk posture and function with greater confidence and agility.