Growing Regional Bank Preempts Potential Cyber Attackers

Chooses Illusive Networks to Reduce Its Attack Surface

Introduction

This regional bank, which offers consumer, business, and online banking services, distinguishes itself by providing the personal touch that huge multinational banks often don't. The bank now aims to increase its client base and maintain customer loyalty by offering digital services such as a mobile banking application, the ability to instantly "turn on and off" their debit cards, and text-driven banking features.

> *"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 Security Director

Challenge

Because this bank is expanding digital services to enhance customer relationships, it needed to:

- Enhance cybersecurity coverage to counter potential new risks
- Increase productivity of a small security team
- Expand security capabilities without increasing management overhead or complexity

Solution

The company deployed the Illusive Networks® solution to detect potential attackers quickly and gain easy-to-use incident investigation tools before attackers could damage the business.

Results

- Improved the bank's ability to identify and investigate potentially malicious activity
- Increased protection without increasing staff or management time
- Gained advanced cyber capabilities on par with those of much larger banks

Challenge - Getting Out in Front of Growing Cyber Risk

Although a growing portfolio of electronic services helps increase customer engagement and loyalty, it also increases the bank's attack surface, which in turn increases the possibility of cyber attacks — and the amount of impact they can have. Despite layered security protection, it's a given that a determined attacker will find a way into the network through social engineering tactics, such as phishing. Once in, he will methodically work to find a path to sensitive financial data or customer information.

"We've always taken security extremely seriously," said the bank's IT security director. "With widespread, targeted attacks, we want to do everything possible to proactively protect our customers' data and assets." The bank's commitment to proactive protection has created a robust enterprise-class security infrastructure, with multiple layers of protection covering endpoints, networks, and connections. But something was still missing.

"When I'd read about reported data breaches, the original intrusion had happened months or even a couple of years before," he said. "It took that long before the organization realized that it had been breached and that bothered me. I wanted to quickly detect and shut down a threat if it managed to breach our other defenses. But a solution also had to be easy to manage since we have a small staff."

Solution - A New View on Protection

The IT manager was invited to a local network security gathering, and there he found his "missing link." He attended a presentation by Illusive Networks on how deception enables APT detection and was very impressed.

"The concept behind Illusive's deception technology is great," he said. "The honeypot approach has been around a long time, but by itself doesn't give you the attacker's view of the network. You have to hope that an attacker finds a honeypot and interacts with it long enough for you to sort through a tide of alerts before knowing how to respond. With Illusive's Attacker View™ map of our network, there is no guesswork."

The bank chose Illusive and deployed it within a few weeks. Illusive creates a rich maze of false data and potential routes to an organization's sensitive assets and spreads it across the network infrastructure.

Even an advanced attacker can't distinguish between real and fake information presented by Illusive, and progressing towards critical assets becomes virtually impossible without being detected.

Using the Illusive Deception Management System™, the bank deployed network, endpoint, data and application deceptions to trip up an attacker anywhere he might land in the network. Deployment was rapid and creating tailored deceptions was surprisingly easy.

"We have a tremendous relationship with Illusive," the IT security director said. "Illusive, working with our vendor's implementation team, made themselves available for regular calls and was concerned to make sure the solution meets our every need."

Empowered Response

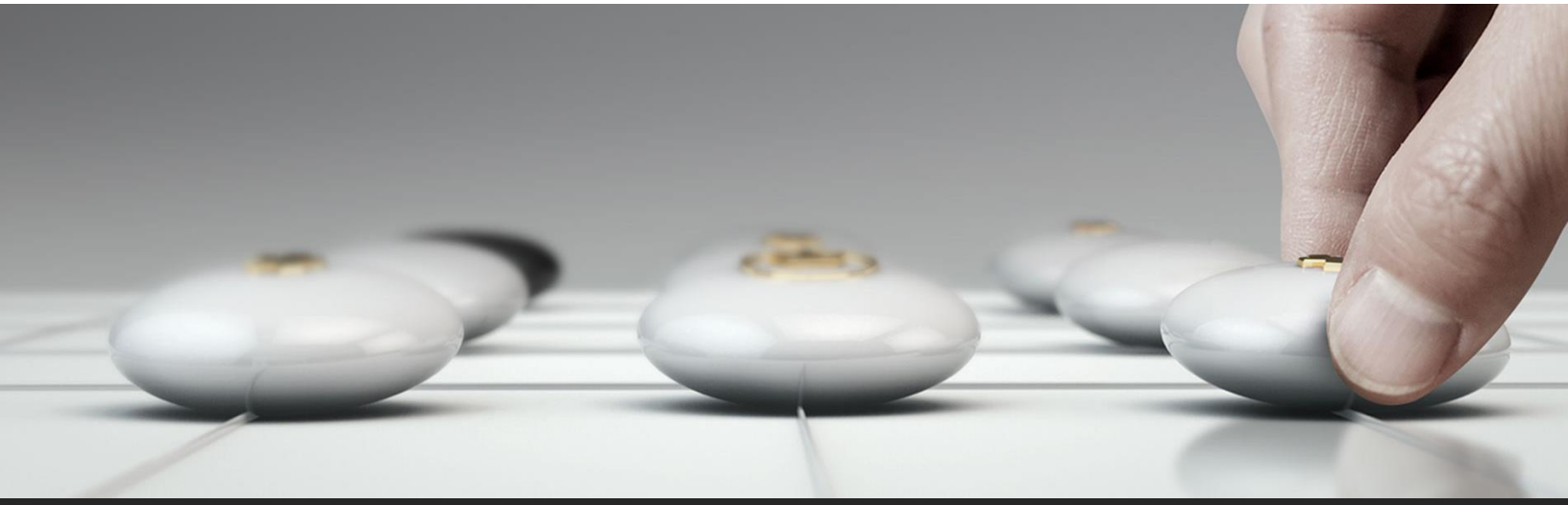
The bank's incident response process was well defined, but Illusive enhances its ability to execute it. Because Illusive deceptions are invisible to valid users, they do not accidentally encounter them and set off false positive alerts. Anyone that encounters a deception is immediately reported as a threat.

Illusive detects attackers with 99% accuracy before they can do damage or move deep into the network. It also provides real-time, source-based forensics that unveil attack location, path, techniques, and context to accelerate incident response.

The high reliability of Illusive alerts allows the bank to immediately treat them as a high priority, improving the efficiency of its valuable resources. "From a detection standpoint, Illusive does our work for us," said the IT manager. "The primary benefit is that we can immediately recognize if an attacker has made it through our perimeter defenses."

Obvious Value, High Assurance

When the Illusive solution was presented to the bank's executive team and board of directors, they immediately recognized its value. Not only does it immediately alert the team of valid threats, it requires minimal management. Illusive makes it possible to acquire threat hunting capabilities equal to - or better than - those of banks many times the bank's size. "Illusive closes the gap between a targeted attack and awareness of an attacker's presence," said the IT manager. "It allows us to proactively protect our customers, business, and assets. It makes my job a lot easier."



About Illusive Networks

Illusive Networks is a pioneer of deception technology, empowering security teams to take informed action against advanced, targeted cyberattacks by detecting and disrupting lateral movement toward critical business assets early in the attack life cycle. Agentless and driven by intelligent automation, Illusive technology enables organizations to significantly increase proactive defense ability while adding almost no operational overhead. Illusive's Deceptions Everywhere® approach was conceived by cybersecurity experts with over 50 years of combined experience in cyber warfare and cyber intelligence. With the ability to proactively intervene in the attack process, technology-dependent organizations can preempt significant operational disruption and business losses, and function with greater confidence in today's complex, hyper-connected world.

Contact Us

- US: +1 844.455.8748
- Outside the US: +972 73.272.4006
- For more information about how Illusive can help lower your APT attack risk, subscribe to our blog and visit us at www.illusivenetworks.com.