Illusive Networks

CASE STUDY

Top US Law Firm

Top Law Firm Builds a Strong Case for Deception Technology

> *“Not only did Illusive meet our three critical requirements, we believe that the entire concept behind the solution is far stronger than other solutions we evaluated.”*
>
> **Director of Technical Operations**

Illusive delivers "inside" visibility for the operations team and reassurance for the firm's clients

The Company

This legal firm ranks among the top 100 law firms in the US. As a full-service organization, it conducts nationally recognized practices in litigation, business law, and government relations. The firm's client list includes global Fortune 500 enterprises, middle-market companies, startups, and high-profile individuals.

CHALLENGE

Identify and respond quickly to lateral movement inside the network

Protect email, document management systems, and confidential client data from compromise

Meet clients' requirements for safeguarding their data

SOLUTION

Illusive Networks
Attack Surface Manager

Illusive Networks
Attack Detection System

RESULTS

Enabled rapid rollout with easy deployment

Gained visibility into assets and network as an attacker sees them to strengthen defenses

Added critical assurance of security posture for the firm and its clients

The Challenge

Trust is important to all business relationships, but for law firms, trust is everything. Clients' strategic business data, personal information, privileged communications, and trade secrets are entrusted to attorneys. As most of this data is digital, it's easily accessible to any attacker who can reach it—and no law firm is too small to be immune from cyber attack. Client IP, business merger plans, financial strategies, litigation evidence, and privileged communications are all valuable on the black market. When law firm clients have audit and regulatory requirements, such as HIPAA and others, by extension the law firm has an obligation to understand and meet those requirements. Often, attackers use a law firm as a vehicle to go after their true target—one of the firm's clients. Threats find their way in via unsecured communications from clients, public file-sharing websites, and unknowingly infected USB drives.

This firm has multiple data centers, hundreds of virtual servers, and regional offices across North America and in Europe. For the past two years, it has built its security team and added new measures to its existing perimeter security infrastructure. Engineers also perform annual vulnerability and pen testing. However, a growing number of clients have begun requiring assurance of the firm's security controls and policies in place as part of their RFPs. Current business insurance policies also require having a certified SOC.

The Challenge (cont'd)

As the team strategized for the future, they realized they had no way of knowing if an attacker was already inside the network moving towards "crown jewel" assets. Crown jewels are the business-critical assets that if they were disabled, lost, or stolen, would compromise the firm's operations, potentially ruin its reputation, or even expose the firm to lawsuits. Client data is a crown jewel, and it can reside across many different systems—archives, email, case management, and document management systems. Billing information, case data, SharePoint files, and electronic communications are also crown jewels that attackers covet.

"For us, crown jewels include email, document management, and phone systems," said the Director of Technical Operations. "When attorneys can't access records, use computer systems, or communicate with clients, firm revenues and client trust are immediately affected.“

The Solution

> *"Illusive strongly complements our existing security infrastructure, giving us unprecedented visibility into any attacker that might evade other controls"*

The team shifted its security perspective to begin assuming that an attacker was already in the network, working to target valuable data. As they began discussing possible solutions, they discovered deception technology and launched an evaluation process. The team studied Attivo, Illusive, and TrapX solutions, narrowing their proof of concept testing to Attivo and Illusive.

"Our security and IT teams are outstanding, but we already have full plates," said the Director of Technical Operations. "For us, the new solution had to be easily manageable. It also had to be reliable, meaning that we only receive accurate, valid alerts. Finally, we needed it to be easily deployable.“

After running the proof of concept with both products, the teams chose Illusive. The Illusive Networks platform is agentless, intelligence-driven technology that effortlessly creates a dense web of deceptions that easily scale across the infrastructure. Featherweight deceptions on every endpoint mimic real data, credentials, and connections that an attacker needs to move within the network. Confronted with a distorted view of reality, it becomes impossible to choose a real path forward. Unknown to the attacker, one erroneous step alerts the security team. With high-fidelity alerts, the team knows that the threat is real and immediate. Illusive then captures forensic data from systems where an attacker is operating and delivers rich, precise incident data in real time for rapid response.

The Solution (cont'd)

Illusive's powerful solution also enables the team to discover and show all pathways that an attacker could use to move through the network toward crown jewels. Prior to deploying deceptions, the team can look at the firm's entire attack surface. They can continuously identify unused or extraneous access privileges, as well as improperly stored credentials that attackers can compromise and use to their benefit.

"Not only did Illusive meet our three critical requirements, we believe that the entire concept behind the solution is far stronger than other solutions we evaluated," said the Director of Technical Operations. "We can see our network and crown jewels just like an attacker would see them and defend them accordingly."

Easy Deployment and Management

The Director and his team worked closely with Illusive Professional Services engineers during the proof of concept and first phase of deployment. Illusive deceptions are placed around crown jewel systems and pathways—ready to detect an attacker so the team can preempt movement and prevent access. As the deployment expands firm wide, other on-premises and cloud-based assets can be brought under deception management.

Getting to Run

"We're taking a crawl, walk, run approach to firm-wide rollout," said the Director of Technical Operations. "This allows us to strategically deploy in a way that complements our existing layers of defense as we expand rollout to more endpoints."

The law firm expects to achieve several important benefits. Illusive provides the ability to manage the firm's attack surface. As the team moves forward, they will begin by identifying extraneous or mis-stored credentials. These can be evaluated or removed and changes reflected in new policies.

"Illusive strongly complements our existing security infrastructure, giving us unprecedented visibility into any attacker that might evade other controls," said the Director of Technical Operations. "At the same time, Illusive is a powerful tool for reassuring clients that we have leading-edge security in place."

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.