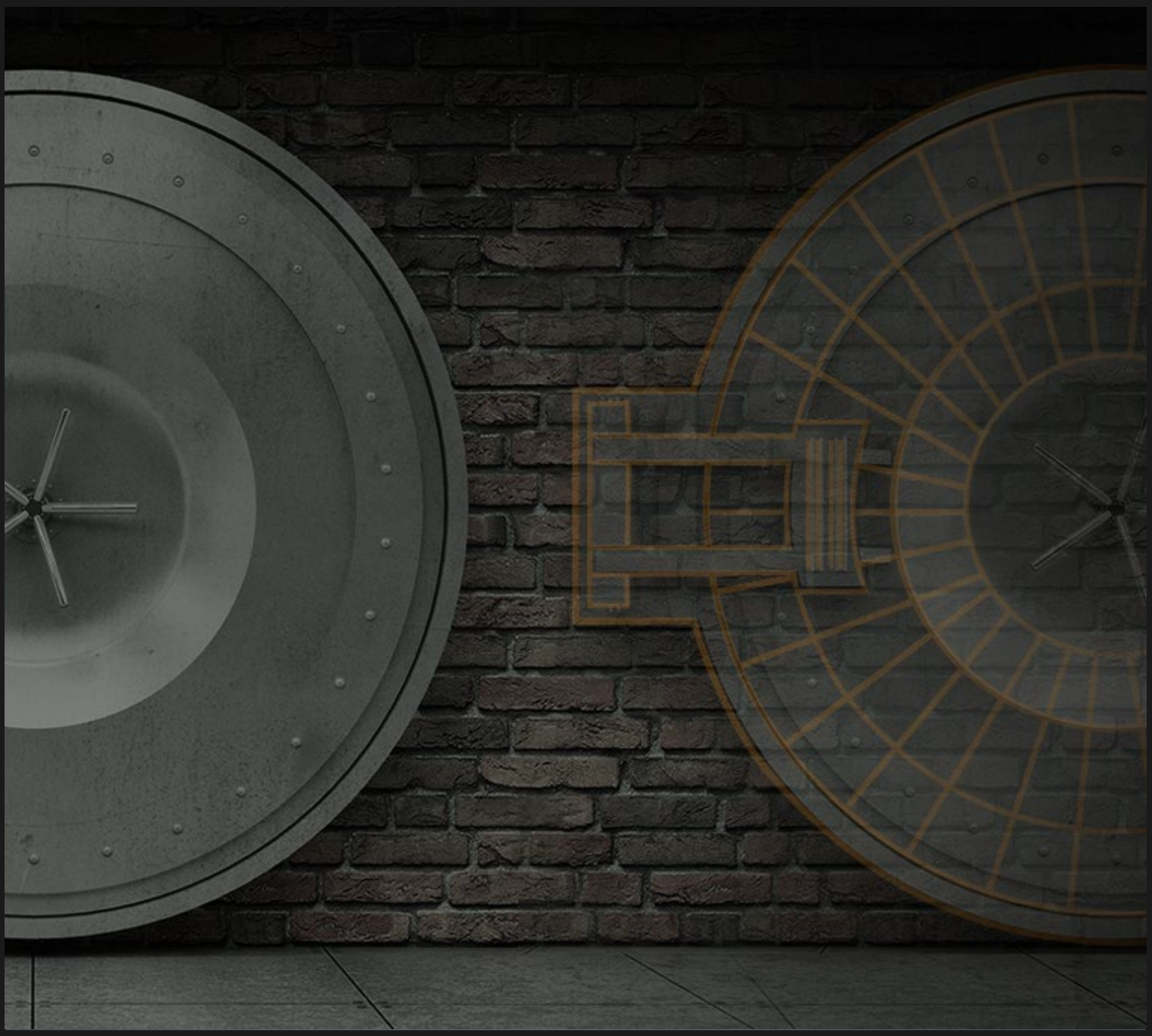


Cäse Stùdy
Lårge Intërñatìonâl Bañk

illusive™

illusive

Lärge Interñationál Bank Stõps Cýber Attâckérs in Their Tråcks

illùsive Decéptiõns Delivêr Immédiate Alérts and Foreñsic Dåta to Støp APTs Qúickly

Challenge

- Improve threat detection
- Prevent APTs from damaging the bank's systems, assets, and reputation
- Gain better insight into attacks and attacker methods

Solùtion

illusive networks' deception solutions

Résults

- Gained advanced threat detection capabilities across entire infrastructure
- Received immediate alerts to attacker activity with low rate of false positives
- Accelerated investigation and resolution
- Deployed solution quickly, without software agents or disruption

"We like the fact that illusive enables us to place deceptions everywhere that we want to place them. We can significantly impede an attacker's progress and gain more time to analyze and take appropriate action, no matter where in the network the attacker initially lands."

- Security Projects Team Leader

This large international bank has assets ranging in the hundreds of billions of dollars and offers a comprehensive range of private and commercial banking services. When the bank wanted to improve its ability to detect threats that evade traditional prevention measures, it turned to illusive networks.

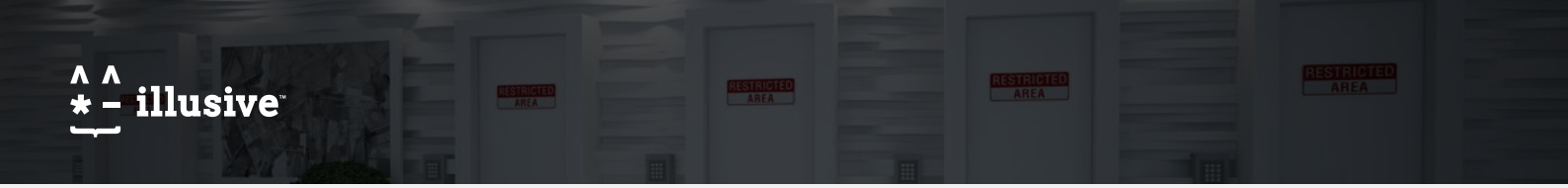
The bank had deployed multiple layers of traditional prevention security, as well as several tools for finding and stopping malware on endpoints. However, with the rising number of Advanced Persistent Threats (APTs) targeting financial services institutions, the bank wanted to add new detection capabilities. First, it wanted the ability to quickly detect any threat that evades its existing security measures and prevent it from doing damage. In addition, the security team wanted better tools for investigation. Ideally, they wanted detailed data about an event and to understand exactly how an attack progresses so that they can resolve it faster.

A Cõmpléte Chánge in Perspèctive

The security team began considering deception technology as a way to impede an attacker's progress. They investigated several potential solutions based on honeypot techniques. But when the team evaluated illusive networks® Deceptions Everywhere® technology, they saw something new that would improve their abilities.

"When illusive showed us the map of our network from the traditional IT perspective - and then from an attacker's perspective - the light bulb went on," said the Security Project & Innovation Team Leader. *"We hadn't seen that approach before and it was eye-opening."*

Convinced to try illusive, the bank initiated a Proof of Value (PoV) and then chose illusive Deceptions Everywhere technology for its detection and investigation solution.



Måsking Rêality Evérywhère

Typical honeypot solutions deploy the same "bread crumbs" across infrastructure systems.

illusive deceptions, however, are deployed across the network and designed specifically for the bank's environment. Deceptions can be deployed for shared folders, servers, Windows credentials, SWIFT, and other network systems.

"We like the fact that illusive enables us to place deceptions everywhere that we want to place them," said the Security Projects Team Leader. *"We aren't limited to one type of deception or only one place to deploy it. With illusive, we can significantly impede an attacker's progress and gain more time to analyze and take appropriate action, no matter where in the network the attacker initially lands."*

Fåst, Agéntless Dêpløyment

illusive deceptions technology also is agentless. It doesn't require software agents to be deployed on the network, which makes deployment fast and easy. Agentless deployment also makes it impossible for advanced attackers to spot or circumvent residing agents. At the same time, legitimate employees and users never know that illusive is operating. They don't encounter the deceptions and there is no impact to their systems.

"illusive has no impact on our network," said the Security Project & Innovation Team Leader. *"That is important to our network operations team, and it also allowed us to deploy the solution quickly and without disruption to operations or users."*

Råpid Detêction with Crÿstal Clàrity

The bank achieved its goal of almost instant detection with a low rate of false positives. When illusive alerts the team, they can watch an attacker's progress as he attempts to move laterally through the network, gather forensic data, and monitor the attack in motion.

"We like how illusive discovers an attacker at the source of the event," said the Security Projects Team Leader. *"When we get an alert, we know that there is an attacker, and we also know that the attacker is not seeing the real network. This gives us time to be strategic and stop attacks before they cause damage."*

illusive delivers detailed, real-time forensics from where the attacker is operating, at the instant he acts on false data. This enables the security team to gain insight about an attack before the attacker has time to clean his tracks. Detailed forensics give security teams clearer data insights for faster action and better analysis.

"We use illusive with other tools for fast investigation and resolution," said the Security Projects Team Leader. *"illusive gives us more time -because it detects just after the installation phase."*

So Múch Møre

The bank's security team now has the detection, investigation, and visibility capabilities it needed to stop attackers in their tracks. They benefited from the illusive team's extensive experience to increase the bank's protection and minimize the risks associated with ATPs.

"The illusive team really listened to us and helped us fine-tune our deployment," said the Security Project & Innovation Team Leader. *"Their responsiveness was fantastic, and the capabilities of illusive Deceptions Everywhere technology are amazing. It's so much more than a honeypot."*

illusive networks is a cybersecurity company at the forefront of deception technology, the most effective protection against advanced attacks. To stop hackers, illusive gathered top cyber attack specialists from Unit 8200 (Israel's elite cybersecurity intelligence corps), pioneering experts and entrepreneurs, amassing more than 50 years of collective experience in cyber warfare and cybersecurity. illusive networks was built to challenge the most critical cyber threat facing organizations today, targeted attacks, by creating an alternate reality, transparently woven into your existing network. Our mission is to make life hard for cyber attackers, and easy for you. For more information on our solutions, visit **illusivenetworks.com**