The Illusive Active Defense Suite and BlueCat Adaptive DNS

Speed Deployment with Automated IP Address Provisioning

Illusive enables customers to deploy an inescapable maze of deceptions that force attackers to unknowingly navigate an environment that mimics the real-world network assets they need to perpetrate an attack—one false step in their lateral movement triggers detection. Generating authenticity of deceptions requires a mix of real network data with markers and the ability to automatically execute refreshment of deceptions on a continuous basis, keeping the 'false' environment ever-dynamic and credible. For example, in strategic intersections of network activity, Illusive will associate a real IP address with a fake Active Directory profile, a task that's typically completed manually. To aid in the ease and productivity of this process, Illusive has built 'out-of-the-box' integration with the BlueCat Adaptive DNS Platform to automatically provision IP addresses to speed deployment. An API token handshake binds the platforms, seamlessly mapping deceptive hostnames.

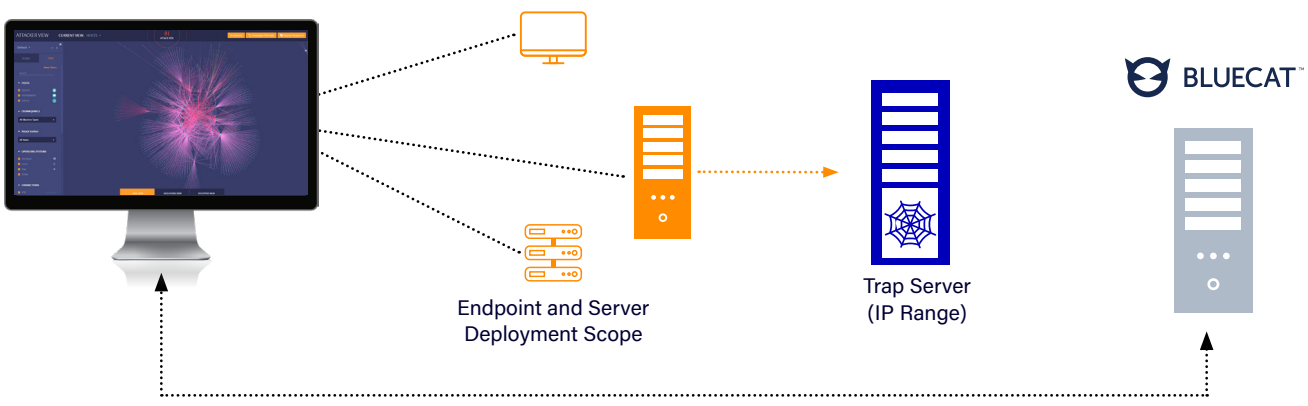
With Illusive and BlueCat working in tandem, your organization reaps the following advantages:

- Streamline the process of IP address provisioning for deceptive artifacts
- Expand scope of deception deployment targets without network conflict
- Enhance deployment efficiency between networking and security teams
- Harden security of DNS configuration mapping

How Illusive & BlueCat Enhance Deception Efficiency & Authenticity

1. Illusive plants hostname deceptions on endpoints across the organization
2. Operation requires DNS mapping (hostname, IP) to bind deceptive hostnames to trap servers

Illusive interacts with **BlueCat** to seamlessly and adaptively map DNS records



Streamline Deception Deployment with Illusive and BlueCat

As a general rule, especially given the constant challenge of insider-based threats, the fewer the number of people who know about a deception deployment, the better. The need for network resources to build out a realistic-looking environment unfortunately runs counter to this goal.

Ordinarily, Illusive needs help from the network team to build out deceptive connections. For every endpoint or strategic junction they protect, they have to request an IP address from the network teams—usually a manual process which slows down deployments and hinders timely expansion to newer areas of the network.

From within the Illusive console, customers can easily configure BlueCat's Gateway automation platform to automatically provision IP addresses for creating deceptive environments. Network admins know that an IP address is assigned and regulate the pool those addresses come from. At the same time, network administrators aren't aware of how the IP address will be used, limiting scope of knowledge to essential personnel only.

Illusive and BlueCat in Collaboration: Key Benefits

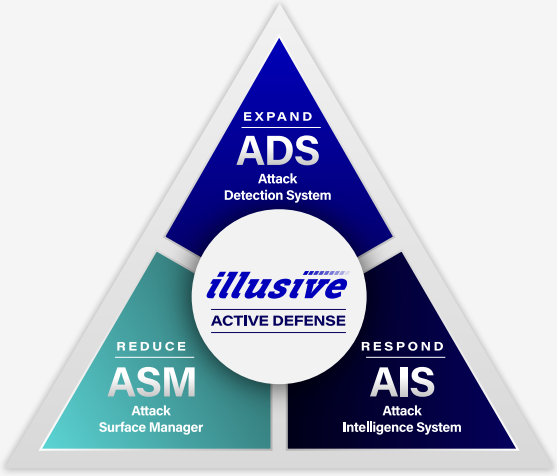
- Ensure dynamic authenticity of Active Directory deceptions
- Enhance operational efficiency and scalability
- Minimize deployment impact to network team resources
- Reduce DNS misconfigurations that create attack risk
- Ensure security of DNS operations

Illusive's Active Defense Suite is a vital part of a diversified detection strategy, filling an important attacker lateral movement detection gap in existing perimeter defenses. Each of the products in the Illusive Active Defense Suite play an important role in preventing attackers from achieving their objectives by creating a hostile environment and accelerating the time to detection for an attacker that has established a beachhead.

Attack Surface Manager (ASM) continuously analyzes and removes unnecessary credentials and pathways, reducing the attack surface.

Attack Detection System (ADS) makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions.

Attack Intelligence System (AIS) delivers human readable on-demand telemetry for current attacker activities to speed investigation and remediation.



About Illusive

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one! To learn more, visit **www.illusive.com**

About BlueCat

BlueCat is the Adaptive DNS™ company. The company's mission is to help the world's largest organizations thrive on network complexity, from the edge to the core. To do this, BlueCat re-imagined DNS. The result – Adaptive DNS™ – is a dynamic, open, secure, scalable, and automated resource that supports the most challenging digital transformation initiatives, like adoption of hybrid cloud and rapid application development. Learn more at **www.bluecatnetworks.com**