The cloud is a non-negotiable part of any given organization's infrastructure and will only grow in importance as more workers move to remote offices and workstations. Illusive Networks Cloud gives organizations the tools they need to scale, increase agility, and maximize productivity without having to compromise on security, impact DevOps or affect cloud service usage.

Secure Pathways to, from and between Clouds
Illusive Networks eliminates the guesswork of safeguarding the cloud, protecting your off-premise deployment with any cloud provider by making your environment hostile to attackers. This is accomplished through a combination of finding and removing the most common attacker paths for moving towards critical data in the cloud and replacing those paths with deceptive versions of the same information meant to entice attackers into engagement. Once attackers interact with this deceptive data, organizations have a high-fidelity evidence that a cloud attack is underway and can instantly take steps to contain it.

Securely Accelerate Your Digital Transformation
Leveraging Illusive attack surface management and deception reduces account takeovers, lowers the mean time to identify and remediate misconfigurations, catches malicious insiders, and closes cloud security and attack surface visibility gaps. Don’t let security worries slow your organization’s digital transformation accelerate it with protection that gives you the visibility to stop attacker movement no matter where it is occurring.

The Benefits of Protecting the Cloud with Illusive:
• Security & threat visibility on any public or private cloud
• High-fidelity account takeover detection in the cloud
• Reliably detect cloud misconfigurations for rapid remediation
• Detect insider threats coming from anywhere
• Quickly deploy cloud-ready, hardware-free decoys
• Highly-authentic server-to-server deceptions
• Expose connections between privileged users on-premise and in the cloud
Illusive Networks for Cloud Security: Key Features

Attack Surface Management in the Cloud: Visualize and automate the discovery of which cloud data is a “crown jewel” that needs to be protected. Find and eliminate common attacker pathways towards critical information. Gain visibility into insecure usage and users on all common SaaS applications, including G Suite, Microsoft 365, Salesforce, and many more.

Privileged Cloud Credential & IAM Violation Discovery: Surface potential privileged identity blind spots and mitigate vulnerabilities created by shadow admins and other extraneous domain users.

Cloud Deceptions: An extensive selection of in-cloud data deceptions that seem like authentic pieces of valuable information to attackers and malicious insiders, tricking them into engagement, and forcing them to reveal their unauthorized presence to defenders in cloud environments. Cloud deceptions include false AWS tokens, deceptive SaaS application data, SSH and RDP deceptions, and much more.

Server Deceptions: Highly-authentic deceptions based on commonly-used web and CI/CD servers, such as Tomcat, IIS and Jenkins servers. These are complemented by a slate of server-to-server deceptions that are designed to find and stop attacker movement between those servers.

Microsoft Office Word and Excel Beacon Files: Organizations can automate the customized creation of hundreds of thousands of deceptive Word and Excel documents. Real and deceptive Word and Excel documents can be also beaconed to immediately alert organizations to the usage of sensitive documents by malicious insiders or external attackers.

Standalone Decoys: Lightweight, hardware-free deceptive systems that can live in the cloud and turn any local host into a decoy that collects insight about attacker tactics and practices with zero additional operational overhead.

End-to-end Microsoft Cloud Tools Support: Out-of-the-box integrations with Azure AD, Intune and Microsoft Managed Desktop (MMD) that allow for full Illusive deployment in Microsoft-enabled cloud environments.

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.

Attacks come from all directions - from phishing emails to cloud account takeovers. The key to foiling attackers is stopping the attacker’s ability to move anywhere they might be.

Stopping attack movement means stopping lateral movement in the data center environment, vertical movement to and from cloud, and movement across and within clouds. Illusive does all three, providing a comprehensive platform for stopping attacker movement no matter where they start or end up.