



illusive®

LogRhythm®

Real-Time Post-Breach Threat Detection and Management Illusive and the LogRhythm NextGen SIEM Platform

Illusive Networks has joined forces with LogRhythm to provide real-time threat detection at breach beachheads while enhancing and automating incident response. Illusive deception delivers high-fidelity alerts that LogRhythm customers can leverage to shrink the time and overhead required to identify, analyze and remediate threats. With the power of Illusive Networks and LogRhythm working together, your organization can increase IR and SOC efficiency, expand threat visibility and ultimately harden your overall security posture.

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



Detect the most sophisticated human attackers, insiders, and malware



Automatic or manual isolation of malicious IPs and hosts



Comprehensive forensic data about attackers and endpoints



On-demand Illusive forensic collection through LogRhythm playbooks

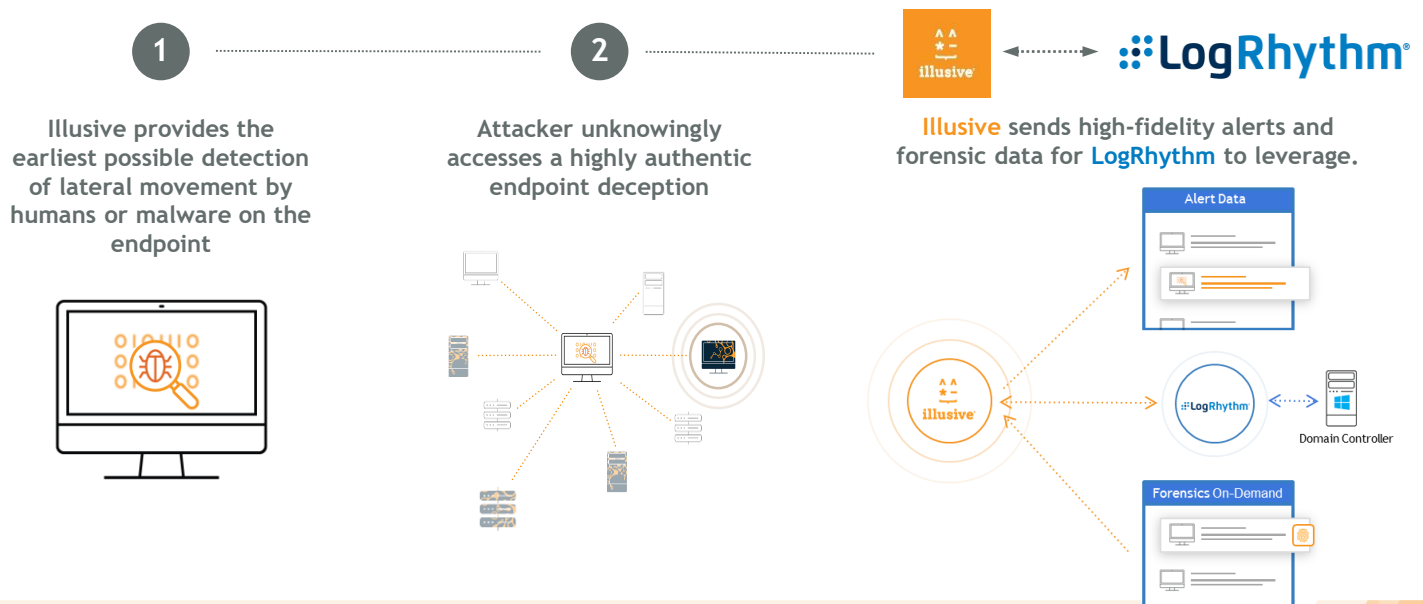


View high-fidelity alerts within LogRhythm



Enable additional deception techniques to harden security

How Illusive and LogRhythm Work Together to Identify and Manage Threats





Early Breach Detection, Powerful Forensics & Expanded Deception

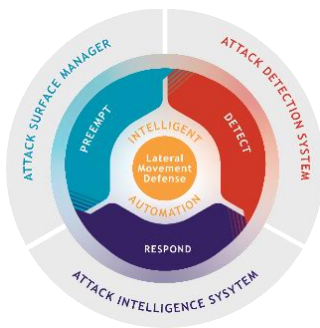
Illusive spreads inescapable deceptions throughout your network that are indistinguishable from the sensitive materials cybercriminals seek to help them move laterally after a breach. 99% of attackers interact with one of these deceptions within three hops from the attack beachhead, providing high-fidelity incident alerts. Rich forensics about threats and attackers get captured and can be automated as an integral part of your LogRhythm playbooks.

LogRhythm also enables additional deception techniques, leveraging the NextGen SIEM Platform's communication with your Active Directory to trick attackers into stealing fake credentials, which then act as a beacon that warns of an attacker's presence.

Illusive and LogRhythm in Collaboration: Key Benefits

- * Detect and isolate attackers early in the threat lifecycle
- * Halt vertical movement between hybrid and multi-cloud ecosystems
- * Amplify the power of limited SOC and IR resources
- * Expand viewable attack data & playbook automation scenarios within LogRhythm
- * Harden your security posture with advanced deception techniques

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.



Preempt: Finds and removes errant credentials, connections, and attack pathways to deter unauthorized lateral movement.

Detect: Forces attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making.

Respond: Enables rapid, effective response and remediation when attackers are present by providing contextual source and target forensics.

ABOUT ILLUSIVE

Instead of building walls and restrictive controls around your assets, Illusive disarms the attacker—destroying their decision-making and depriving them of the means to reach their targets.

It's a simple, adaptive approach that empowers your defenders to stop cyberthreats that could otherwise dwell in your environment for months or years.

Built on agentless, intelligent automation that requires very little IT coordination, Illusive immediately shifts the advantage to your defenders—and frees them from the complicated, noisy, data-heavy approaches that burden them today.

ABOUT LOGRHYTHM

LogRhythm is a world leader in NextGen SIEM, empowering thousands of enterprises on six continents to successfully reduce cyber and operational risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines advanced security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation and response (SOAR) in a single end-to-end solution. LogRhythm's technology serves as the foundation for the world's most modern enterprise security operations centers (SOCs), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won countless customer and industry accolades. For more information, visit logrhythm.com.

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.