

Prevent, detect and stop.

# Eine feindliche Umgebung für Angreifer

## Erschaffen von Verteidigern, für Verteidiger

Illusive hat weit über 100 der fortschrittlichsten und aggressivsten IT-Angriffsteams der Welt geschlagen! Wie? Die Illusive-Plattform wurde von Menschen entwickelt, die mit nationalstaatlicher Cyber-Aufklärung und -Verteidigung vertraut sind und ein taktisches Verständnis dafür haben, wie Angreifer operieren. Die drei Kernelemente von Illusive wurden entwickelt, um Ihnen dabei zu helfen reale Bedrohungen einfach und leicht zu identifizieren, Angreifer zu lähmen und sie auf ihrem Weg zu stoppen.

Cloud Security • Insider Threat Defense • M&A Security • SOC Efficiency • Unsecurable System Protection

### Fortwährendes entfernen von Angriffspfaden

Kontinuierliche Minimierung der Angriffsfläche.  
 Verbesserung der Cyber-Agilität.

Der Attack Surface Manager (ASM) beugt Angriffen vor, indem er gespeicherte Anmeldedaten, nicht getrennte Verbindungen und Sitzungen identifiziert und entfernt. Denn genau diese Wege nutzen Angreifer, um sich in einem Netzwerk zu bewegen. Eine saubere Umgebung verwehrt Angreifern die Möglichkeit, sich vorwärts zu bewegen.



### Ihr Netzwerk wird zur Falle

Angreifer im Einfallstor aufspüren und stoppen, bevor Schaden angerichtet werden kann.

Das Attack Detection System ersetzt die echten Daten, die von ASM gefunden und entfernt wurden und flutet das Netzwerk mit falschen Daten, die genau das authentisch imitieren, was die Angreifer zu sehen erwarten. Sie werden also zwangsläufig auch mit diesen Daten versuchen, sich im Netzwerk zu bewegen. Und somit Ihre Anwesenheit zu enthüllen.



### Reaktion mit Echtzeit-Daten

Während einen Angriffes, schnelle und effektive Entscheidungen treffen

Das Attack Intelligence System tritt in Aktion, wenn eine Falle ausgelöst wird. Sie liefert umfangreiche, forensische Daten, wie z.B. den Standort des Angreifers, lokalisiert den Ursprung und die Art der Verletzung und leitet diese Daten direkt an ein SOC weiter. Dies verkürzt die Ermittlungszeit um zwei Drittel.



Illusive Networks stoppt Cyberattacken, indem es die Fähigkeit der Angreifer zerstört, sichere Entscheidungen zu treffen, wenn sie versuchen, sich auf ihre Ziele zuzubewegen. Mit Illusive eliminieren Unternehmen risikoreiche Pfade zu kritischen Systemen, erkennen Angreifer frühzeitig im Angriffsprozess und erfassen forensische Daten in Echtzeit, die die Reaktion auf Vorfälle fokussieren, beschleunigen und die Widerstandsfähigkeit verbessern. Durch eine einfache, agentenlose Technologie bietet Illusive flexible, benutzerfreundliche Lösungen, mit denen Unternehmen ihre Anfälligkeit in Bezug auf Cyberrisiken kontinuierlich verbessern können.