Securing the New Normal

How Illusive Networks can help you strengthen security in an increasingly uncertain world

This moment brings together the dangerous nexus of three threat forces that when combined shake the already rocky foundations of global cybersecurity.

Insider threats spike as opportunities increase

Working from the privacy of home, separated physically and emotionally from company and colleagues, those facing increased temptation due to financial hardship, greed, or anger are emboldened. With defensive systems weakened, the opportunity increases for employees with ill-intent to gain enhanced access and privileges undetected.

Altered user activity nullifies baseline patterns

In the new abnormal, defenses relying on detecting anomalies, behavior, access, or virtually any other characteristic are rendered null and void. Customers are reporting 300%+ increases in SOC alerts as these systems misfire due to environmental chaos.

Work-from-Home Expands the Attack Surface

The business continuity imperative to support WFH has exploded the attack surface – with BYO devices, thousand-fold increases in VPN/VPI usage, split tunneling, SaaS applications access over insecure networks, rampant password reuse, loss of physical device control, and a lack of attack surface visibility.

In the face of this weakness, organized attackers are aggressively increasing the intensity and frequency of attacks. This turbulence allows threats to more easily breach perimeter defenses and land inside the network. By creating a hostile deceptive environment that stops attacker movement from anywhere to anywhere, Illusive offers an effective and permanent defensive approach to mitigate all three of these threat forces.

www.illusivenetworks.com
info@illusivenetworks.com

Regain Visibility & Control of the Attack Surface

Illusive finds and maps endpoints wherever they now physically reside and however they are connected; gathering critical data regarding credential safety, newly expanded attack pathways; and most importantly enabling the security team to establish and continuously maintain baseline hygiene controls.

Detect Attacker Movement to and from Anywhere

Since deception does not rely on patterns or behavior, rapid environmental change has no effect on detection efficacy. Detection is based on the simplest of algorithms – either the attacker interacted with a deceptive element or did not. Massively distributed, highly authentic deceptions force attackers to unknowingly interact to progress their attacks in any direction and in the cloud. Only those navigating the underside of the network encounter deceptions. When an Illusive notification fires, it's not white noise—this incident requires immediate investigation.

Catch Insiders Red Handed

Illusive has proven to be a simple and effective insider threat mitigation tool by taking a two-pronged approach. Illusive first ensures that users do not have unauthorized credentials and connections that could be used to access critical assets. Then, tailored deceptions that even the most sophisticated insiders cannot distinguish from real, trigger when the insider's lateral movement attempt is detected, and real-time source forensics deliver incontrovertible proof of malicious intent.