illusive

Insurance Industry Under Attack

What do attackers want?

Insurance companies hold billions of dollars worth of commercial and personal data. As cyberattacks are becoming more frequent across all sectors of the global economy, the insurance industry is experiencing increased numbers of attacks that seek social security numbers, healthcare codes, medical histories, and other valuable personal data.

In 2015, 80 million personal data records were stolen from a leading health insurance company in the US.

What are the cyber defense challenges?

Insurance networks are structured to support multiple complicated products that interact with numerous third parties. Networks often consist of many distributed hosts, numerous sensitive assets, virtual desktops, mobile applications, non-technical users, segregated hosts (without internet access), and different access rights for employees, contractors, customers, and visitors.

With so many access points and so much third party integration, attackers penetrate network defenses by exploiting compliance issues and access rules, or by using targeted attacks (such as spear-phishing campaigns). Once inside, they diligently explore a network via lateral movements, seeking hosts that store sensitive information.

What are the key steps to build a defense strategy?

1. Identify threat actors and build an adaptive strategy to address the varied skill levels of attackers.
2. Maintain a cost effective perimeter defense against common attacks.
3. Prepare a strategy to deal with APTs, wherein sophisticated attackers, having penetrated your perimeter, seek a target on your network.
4. To ensure speedy risk-mitigation and containment, invest in an early detection solution with strong Incident Response capabilities.

What would minimize the risk?

As persistent attackers will always find a way to penetrate your defenses and access your network, risks are minimized by feeding attackers false information and detecting lateral movements before sensitive data is reached.

Attacker View™ by illusive networks reveals your network as an attacker sees it, enabling you to enhance security around potential attack vectors. Lateral movement by the attacker triggers a high fidelity event and allows you to identify attack tools via real time, with source-based forensics. Using the delivered network insights, you can adapt your defensive strategy to real risks without impacting business processes.