TAG Cyber

Security Annual

3RD QUARTER 2023

CYBERSECURITY IN OUTER SPACE UNPREPARED?

ARTICLES / OPINIONS / INTERVIEWS

AN INTERVIEW WITH ALEX HARRINGTON
CO-FOUNDER AND CEO, SECURECO

STEALTH-BASED NETWORK SECURITY AND DATA PROTECTION

In the face of rising cyber threats, traditional network security measures often fall short. SecureCo, however, is redefining the rules of the game with its innovative security solutions. Using stealth, obfuscation, and encryption techniques, SecureCo protects internet connections by reducing the attack surface and emphasizing proactive security measures. This innovative approach has positioned them at the cutting edge of the cybersecurity landscape. Our recent discussion with SecureCo explored network obfuscation and how it bolsters defenses against diverse cyber threats. Furthermore, we discussed the implications of revolutionary technologies like generative AI and quantum computing on their approach to security. SecureCo's forward-thinking solutions provide robust protection in the present and lay the groundwork for navigating the future complexities of cybersecurity.

TAG Cyber: Why is SecureCo technology different from typical network security?

SECURECO: The principal difference is that we introduce stealth and obfuscation elements alongside traditional encryption security to secure internet connections. Obfuscation makes the endpoints and data-in-transit much harder to discover, target, and exploit, reducing an organization's overall attack surface. A smaller attack surface reduces vulnerability, risk, and administrative overhead, ultimately reducing financial losses from fraud, breaches, or downtime.

A second key difference is an emphasis on protecting internet data transit. As threat actors become more sophisticated, and the untrusted internet becomes increasingly dangerous, simple encryption is not enough to protect critical data against common exploits. SecureCo protects against monitoring and packet analysis threats —key elements of hacker reconnaissance—and exploits, such as man-in-the-middle, which can result in obstruction, eavesdropping, or data theft.

One more notable distinction is the emphasis on preemptive security, which is currently not in vogue. In an era of budget constraints, the return on investment (ROI) for reactive security, like detect and respond systems, is easily measured by tallying the number of flies caught in a fly trap. However, reactive solutions don't deter attackers or prevent the breach in the first place.

TAG Cyber: What cyber threats does network obfuscation protect against?

SECURECO: Network obfuscation includes a variety of tactics designed to make network assets and data less exposed to attacker discovery,

Generative AI and quantum computing are seismic technology shifts that will yield unexpected results. There are some pretty clear near-term consequences to these emerging technologies, and SecureCo's technology can help companies navigate these changes.

reconnaissance, and exploitation. It works with traditional security approaches in a defense-in-depth strategy to reduce cyber risk and prevent costly incidents.

Attack surface reduction is one notable form of protection. SecureCo's method of establishing connections permits networks to operate in a connected state with no ingress ports open.

Eliminating the open ports is vital since they are a key element that attackers use to identify vulnerabilities, potentially providing an accessible exploitation pathway. Fewer open ports and reduced attack surface lower network security incidents (including initial access breaches) and avert disaster scenarios.

Network obfuscation also protects internet data transit. Nowadays, most data communications are encrypted, but this does not provide complete protection. Adversaries can still observe encrypted data flows, perform reconnaissance, and potentially monitor, intercept, redirect, or obstruct data. Obfuscation can disguise data flows and remove attribution, routing evasively to make targeting and exploitation much harder.

TAG Cyber: What are the most common enterprise use cases for network obfuscation? How widely adopted is it?

SECURECO: Military and intelligence applications have used network obfuscation for at least a decade, but only in the last few years has it been widely available for commercial adoption. Obfuscation can enhance security in common enterprise use cases, including remote access, campus networking, and cloud connectivity. SecureCo solutions can replace VPNs, supplement SASE elements (such as SD-WAN), or provide a more flexible and lower-cost alternative to dedicated telco connections. However, the use case receiving the most enterprise interest and adoption is API security, particularly for public APIs used by mobile apps.

Mobile app APIs are publicly accessible, and attackers attempt to exploit them by mimicking the API calls from the app. Brute force and credential stuffing attacks are common methods of hijacking customer accounts, resulting in financial losses, regulatory penalties, and customer dissatisfaction. Current mitigation tools like WAFs and bot detection software have not fully met these challenges. SecureCo's network obfuscation solution allows enterprises to establish a private connection between their consumer apps and the associated APIs, eliminating bot attacks from side channels.

TAG Cyber: What benefits does SecureCo's network obfuscation have relative to conventional security approaches?

SECURECO: Network obfuscation is part of a defense-in-depth security strategy. SecureCo solutions complement almost all traditional security methods, and we recommend a layered

approach. When going into battle, you still want your armor and shield, but wouldn't you also want an invisibility cloak if it were available? Network obfuscation provides the closest thing you can get to internet invisibility.

Some distinctive aspects of our solutions are beneficial to the customer. First, SecureCo hosts its data delivery platform as a managed service. Our approach to attack surface reduction and data security is mainly set-and-forget. Many cybersecurity solutions are powerful tools, but organizations need a team to manage them, which inflates the cost of ownership and lowers ROI. Not so for SecureCo solutions.

Another benefit to customers is the reduction of network security incidents accompanying the deployment of our network obfuscation solution. This approach minimizes cyber risk and averts expensive breaches while significantly reducing the overhead of logging, investigating, and mitigating the overwhelming influx of incidents.

TAG Cyber: How will emerging technologies like generative AI and quantum computing drive the adoption of obfuscation security like that provided by SecureCo?

SECURECO: Generative AI and quantum computing are seismic technology shifts that will yield unexpected results. There are some pretty clear near-term consequences to these emerging technologies, and SecureCo's technology can help companies navigate these changes. Generative AI can do many things, including creating incredibly realistic human simulacra. In the same way AI can create deepfake videos or emulate a pop star's singing voice, it can also replicate human behavior and fool software designed to prevent bot attacks. This capability will make it much harder to defend authentication APIs in traditional ways. However, SecureCo's approach, which conceals the API endpoint and denies access to attackers, is not vulnerable to these AI-enhanced threats.

Quantum computing presents significant possibilities and challenges. Common encryption will be rendered useless against quantum computer decryption capabilities. It's highly probable that threat actors are stealing high-value encrypted data and storing it for the near future when quantum decryption is available. Quantum-proof algorithms are still in development, so there is no foolproof method to protect against this. However, SecureCo's network obfuscation uses de-attribution, evasive routing, and other methods to make it hard for adversaries to target and harvest customer data. The "store now, decrypt later" threat is mitigated by making customer data hard to find and identify.