BLACKCLOAK™

NETWORK SECURITY FEATURES

BlackCloak performs weekly penetration testing and regular scans of your home networks to detect malware, botnets, and other security issues, and to prevent decisions your children and family make online from resulting in a compromise.

BotNet Scanning of Homes

We scan threat intelligence databases for your home IP address to determine if any devices inside the home have been or are currently communicating with known malware servers, and help remediate this vulnerability as necessary.

Home Network Scans (Penetration Tests)

Each week, we provide external network penetration tests of the public IP address for your home network, scanning for open ports that make your devices accessible to the Internet (e.g., security cameras, home automation systems, routers, etc.), and thus vulnerable to compromise. We also help remediate this vulnerability in real-time as necessary.

WiFi Scanner

The BlackCloak app continuously analyzes network connectivity on mobile devices. In doing so, we detect malicious WiFi hotspots commonly deployed by hackers to breach your data and eavesdrop on your confidential communications (Commonly known as man-in-the-middle attacks). You will receive real-time alerts whenever risky connections are established. These urgent notifications prompt you to immediately disconnect from a rogue network before the hacker can compromise your device.

Deception (Honeypot Technology)

By creating a fake service (often called a honeypot) within the BlackCloak application, we can distract potential attackers. The fake service is designed to be attractive and draw them to it when they first try to access your computer. It looks like an application that might house your sensitive data, and the moment they scan it, we will detect them. Because it alerts us before they even have a chance to take action, it gives us an early warning, allowing us to stay a step ahead of them before they can breach meaningful data.