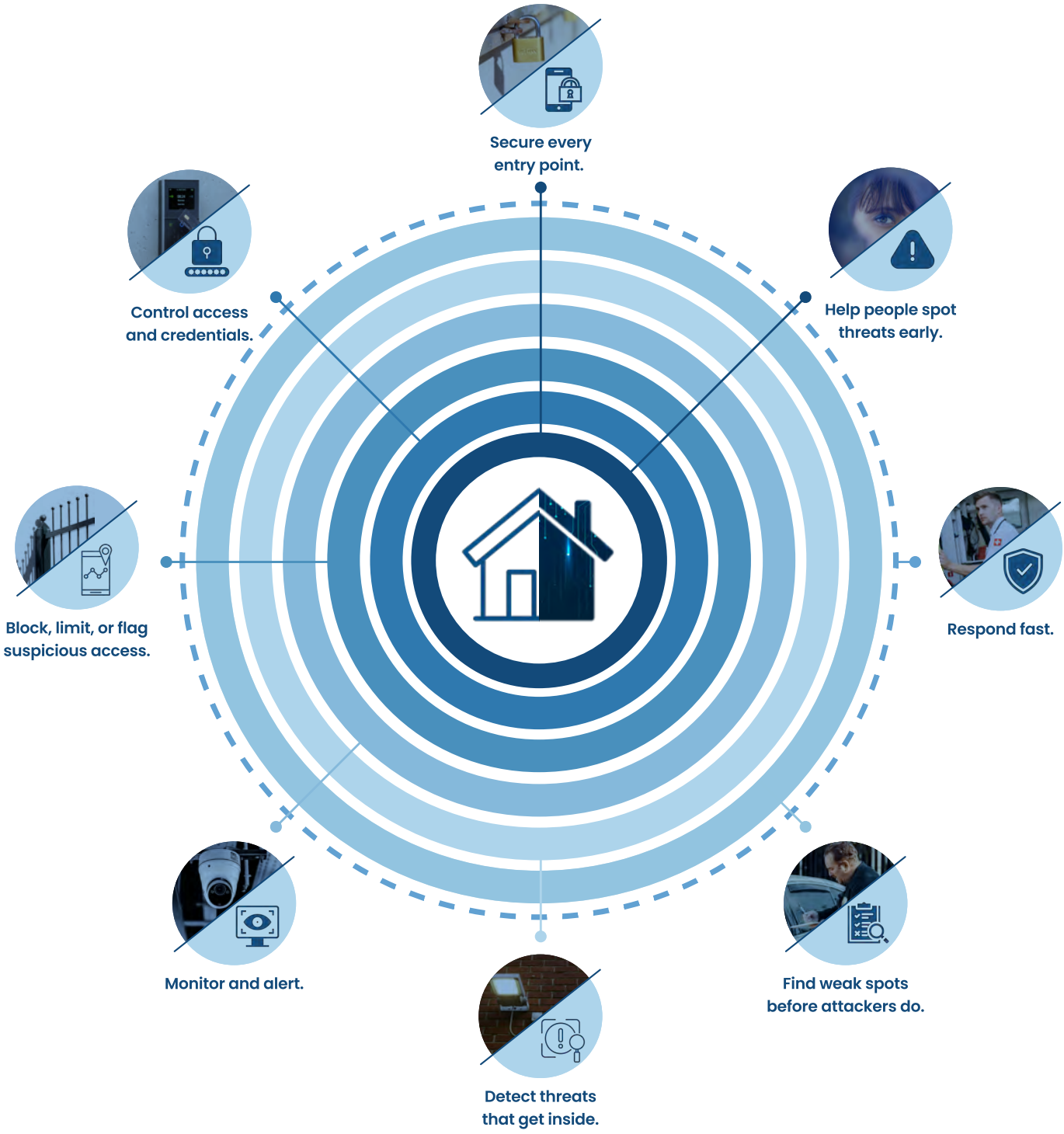
Cybersecurity/Home Security Analogy

1. **Concentric Circle Diagram Content** - A connected home needs layers of protection, just like a physical home.

> Defense in depth means using multiple layers so one safeguard does not have to do the whole job.



2. Side-by-Side Comparison Chart

Physical Home Security	Cybersecurity Equivalent	What it Means
Locks on doors and windows	Secured devices	Every connected device is a possible entry point. Devices need to be set up securely, kept updated, and moved off default settings so they do not become the easy way in.
Alarm code and entry control	Passwords, MFA, access control, and Dark Web/ credential monitoring	Not everyone should be able to enter, and not everyone should have the same level of access. Strong passwords, multi-factor authentication, and user-based permissions help control who gets in and what they can reach. Dark Web monitoring (credential monitoring) adds another layer by alerting you if usernames or passwords tied to the household are exposed, much like finding out your alarm code or spare key has fallen into the wrong hands.
Gate, fence, and property boundaries	Firewall, secure remote access, and geofencing	A good perimeter helps stop trouble before it reaches the house. In cybersecurity, the firewall and secure remote access tools help filter out bad traffic and reduce unnecessary exposure. Geofencing adds another layer by blocking or flagging access attempts from locations that should not be trying to connect in the first place.
Security cameras and monitored security alerts	Monitoring and threat intelligence	Cameras help keep watch and show when something unusual is happening. Cyber monitoring does the same thing by watching activity, generating alerts, and helping a monitoring team determine whether something is routine or a real threat that needs attention, much like a glass-break detector alerts a security monitoring team to a possible breach through a window.
Glass-break detectors and motion sensors	Intrusion detection and endpoint protection	If someone gets past the perimeter, you still want to know what is happening inside. These tools help detect threats already in the environment and can help stop them before they spread.
Security inspection	Vulnerability and risk assessments	A home can look secure and still have weak locks, blind spots, or outdated equipment. Regular cyber assessments help uncover weak settings, exposed devices, and other risks before an attacker finds them.
Emergency response plan	Incident response support	A monitored home-security system does more than sound an alarm. It sends the alert to a security company that can verify the issue and contact police when needed. Cyber incident response works the same way: when something suspicious happens, the right people are alerted, the issue is investigated, and action is taken quickly to help contain the problem..
Knowing who to trust	Awareness training	Even a well-protected home can be compromised if someone opens the door to the wrong person. Awareness training helps users recognize phishing, scams, impersonation, and other social-engineering attempts.

Just like physical security, cybersecurity works best when every layer works together.

SpecOp's Cyber Protect product helps secure the digital home with layered protection for devices, access, monitoring, and response.