Cybersecurity That Works—Without Guesswork

SpecOp Secure

Real Protection. Flexible Models. Recurring Revenue.

Why Integrators Can't Ignore Cybersecurity

The moment you power up a client's network, you share the liability. If a breach happens and you never offered protection, you're the first call—and sometimes the first name in a lawsuit.

Bottom line

- Protect **your business** from breach blame.
- Protect **your client** from real-world threats.
- Protect **your revenue** with monthly RMR.

Choose the Tier That Fits the Job

Cyber Sentry

Entry-level cyber defense

Key Protections:

Endpoint protection (EDR)
Blocks attacks on computers in real time by stopping malicious behavior before it spreads. *(Up to 3 PCs and 3 mobile devices)*

Password vault
Secures passwords and alerts on exposed credentials to help prevent account takeovers. *(Up to 3 users)*

Dark web monitoring
Alerts if usernames/passwords show up in criminal leak sites. *(Up to 3 users)*

Cyber Centurion

Cyber defense with firewall protection + annual risk review

Includes everything in Cyber Sentry plus:

Secure remote access (VPN)
Encrypted connection for home, office, or travel so remote sessions aren't exposed.

Managed firewall protection
Blocks known bad traffic before it reaches devices on the network.

Annual network vulnerability + risk assessment
Yearly check for weak settings/outdated devices, with an action list in an executive summary you can present to the client.

Cyber Protect

Full-scale managed cyber protection

Includes everything in Cyber Centurion plus:

Quarterly network vulnerability + remote risk assessments
Regular checks for weak settings/outdated devices + action list presented to your client by one of our SMEs.

Secure remote access (VPN/SASE)
Encrypted access plus policy-based controls (role-based access, MFA/passkeys, tighter limits on what users can reach).

Managed firewall protection
Blocks known bad traffic before it reaches devices.

AI-driven threat intelligence with Cisco Talos
Automatically updated filtering with protections against common threats (phishing, malware sites, botnets, exploits, and more).

Intrusion detection + prevention (IDS/IPS)
Detects and blocks common attack patterns at the network edge.

Geofencing
Limits or flags suspicious traffic based on geographic location.

Credential & access control
Unique accounts, role-based permissions, provisioning/deprovisioning, MFA/passkeys.

Incident response access
Direct line + playbooks.

Awareness training
Short, targeted training to reduce phishing/scam risk.

Cyber Protect +

Concierge-Level Security

Includes everything in Cyber Protect, plus optional upgrades for high-compliance projects:

Email domain protection & encryption
Deters impersonation of client email addresses and encrypts sensitive outbound messages when required.

Identity management with MFA & passkeys
Adds multi-factor authentication and modern passkey options on top of centralized account control.

Mobile threat defense
Shields phones and tablets from malware, phishing, and unsafe Wi-Fi.

24/7 threat monitoring (MDR)
Security operations team watches the network around the clock, detects threats, and responds as needed.

Activity logging & analysis (SIEM)
Collects and reviews system activity to identify suspicious or hidden patterns.

Continuous posture improvement
Monthly adjustments and targeted hardening to close blind spots before they're exploited.

Data privacy & data broker removal
Removes or reduces personal data exposure on broker sites and deletes compromised records when possible.

On-site assessment
In-person review of homes, offices, and networks with a consolidated findings report.

Data loss prevention (DLP)
Controls and blocks sensitive files, emails, and exfiltration attempts.

Attack surface scanning
Continuous checks of cloud accounts, web apps, and services to find exposed vectors and misconfigurations.

Start clients at the right tier now, then upgrade as risk and expectations grow.

Why Your Clients Need Managed Cybersecurity

Smart-device sprawl:
Every thermostat, lock, and camera is a new attack point.

Basic firewalls fail:
Phishing, credential theft, and malware are built to slip through.

Built-in tools
(Nord, Defender, McAfee) encrypt traffic but don't block malware or exploits.

What You—and Your Clients—Get

- **Always-on protection** threats blocked before clients notice
- **Built-in RMR** monthly revenue on every install
- **Integrates with any client network** fits into the current setup
- **Less firefighting** more billable hours, happier techs
- **Tiered service** Start core, upgrade as risk grows
- **Turnkey install** preconfigured and ready to deploy

Why Integrators Work with SpecOp

- **Designed by Engineers** Network and security specialists build every deployment right the first time.
- **Unlimited Remote Support** Issues resolved proactively, often without even needing to roll a truck.
- **In-House NOC (Network Operations Center) + Incident Response Team** Around-the-clock monitoring, proactive defense, and live incident response.
- **Boost Client Trust** Reliable, secure systems mean fewer panicked calls and longer-term relationships.
- **Real RMR Models** Cyber tiers, NaaS, HaaS, cellular amplification systems as a service—choose, bundle, scale.
- **Proven, Trusted Partner - 20+ Years Securing Custom-Integration Networks** 20+ years protecting luxury homes and commercial sites. We know what breaks, why it breaks, and how to prevent it.

Scan to Learn More

Let's Secure Every Install—Together.

Breach-proof systems, recurring revenue, zero guesswork.
Bring us your next project and see how Cyber Protect fits.

877-770-0767
sales@specopsecure.com
specopsecure.com

Scan for Appointment