

The background of the slide features a blurred image of a white SCW device, possibly a security camera or sensor, with the SCW logo visible on its side. The image is overlaid with a large, stylized orange and blue geometric shape that frames the title text.

2026 Security Budget & Planning Guide: From Audit to Execution

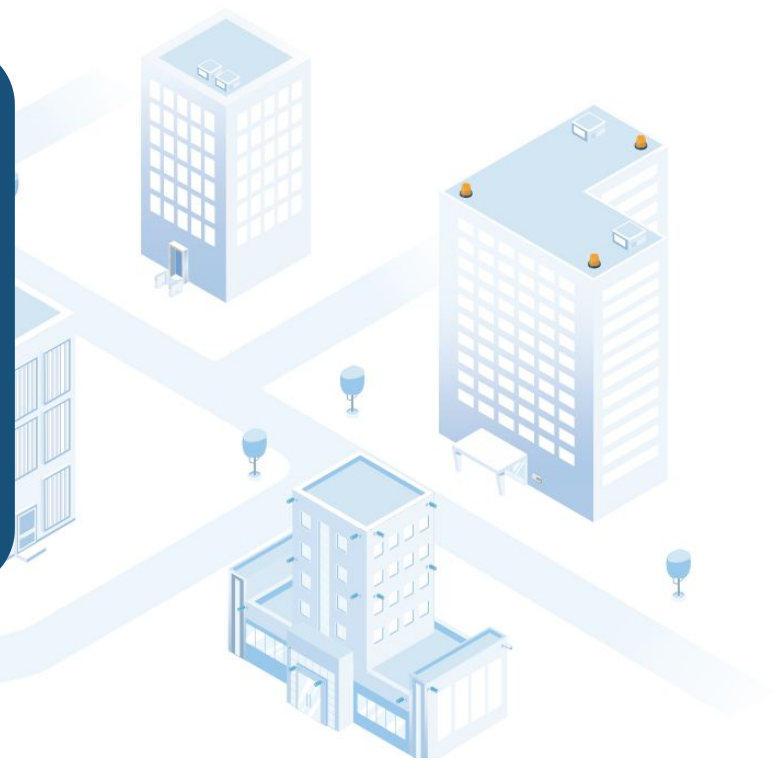


What's in This Guide?

1. **2025 Trends**
 - That Will Shape Your 2026 Security Plan
2. **Step-by-Step Security Audit Checklist**
 - Audit your security system with a ready-to-use template to track your progress.
3. **Smart Security Budgeting for 2026**
 - Where to spend your first security dollar for maximum impact.
4. **Ongoing Monitoring, Maintenance & Optimization**
 - A security system is only as strong as its upkeep.
5. **Security Beyond Hardware**
 - Go Beyond Passive Security with SCW Services



2025 Trends That Will Shape Your 2026 Security Plan



2025 Trends

Workforce Disruption Increased Physical-Security Risk

Layoffs, hiring freezes, and budget pressure throughout 2025 reduced onsite staffing and supervision - forcing organizations to replace human oversight with technology-driven security.

Key Insights:

- Fewer employees onsite means less informal supervision and more security blind spots
- Labor reductions increase stress, mistakes, and missed incidents
- Organizations are under pressure to do more with fewer people

What This Means for Security:

- Fewer guards and staff = greater reliance on automation and analytics
- Manual monitoring becomes unsustainable at scale
- Security investments shift toward technology that reduces labor cost without reducing coverage

2025 Trends

Remote & Hybrid Work Reshaped Facility Vulnerability

2025 saw record levels of remote and hybrid work, leaving facilities less occupied - and forcing security teams to manage sites remotely with fewer people and tighter budgets.

Key Insights:

- Hybrid work rose to ~24% of all U.S. job postings in 2025
- Remote work increases physical-security blind spots & safety incidents
- Reduced onsite presence heightens access and asset risks

What This Means for Security:

- With fewer employees onsite:
 - More unmonitored zones
 - Longer detection delays for incidents
 - Less informal guardianship (the “someone would notice” effect)
- Remote guarding, cloud-based VMS, and mobile access control move from optional to essential

Economic Stress Shifted Crime Patterns

Economic pressure doesn't always increase overall crime but it does increase opportunistic theft and localized property crime, especially where staffing and supervision are reduced.

Key Insights:

- Property crime increases correlate with local layoffs and reduced staffing
- Opportunistic theft targets lightly monitored sites
- Businesses cannot rely on regional or national crime averages

What This Means for Security:

- Static security plans based on historical crime data fall short
- Automated detection, video verification, and perimeter analytics become critical
- Verified alerts and documented incidents matter more as response requirements tighten

2025 Trends

Security Technology Transformed in 2025

2025 marked a shift away from hardware-first security toward analytics driven, integrated systems designed to replace manual monitoring and reduce operational cost.

Most common investments in 2025:

- AI video analytics (fewer false alarms, faster decisions)
- Cloud / hybrid VMS for centralized oversight
- Unified access control + video (single source of truth)
- Remote guarding to replace or reduce physical guards

What This Means for Security:

- Security platforms move from recording video to interpreting events
- Analytics enable faster response with fewer people
- Systems must talk to each other to reduce friction and risk

Summary

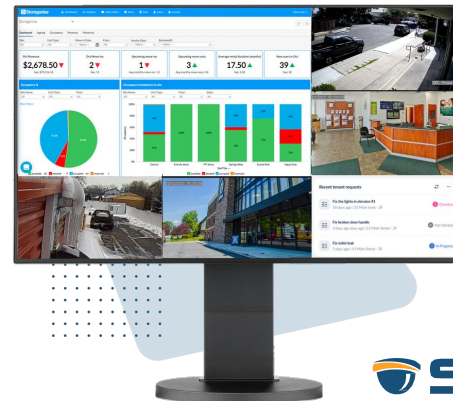
Why 2026 Requires a New Security Approach

By the end of 2025, one reality became clear: security strategies built around people, silos, and manual monitoring no longer scale - especially under budget pressure.

What This Means for Security:

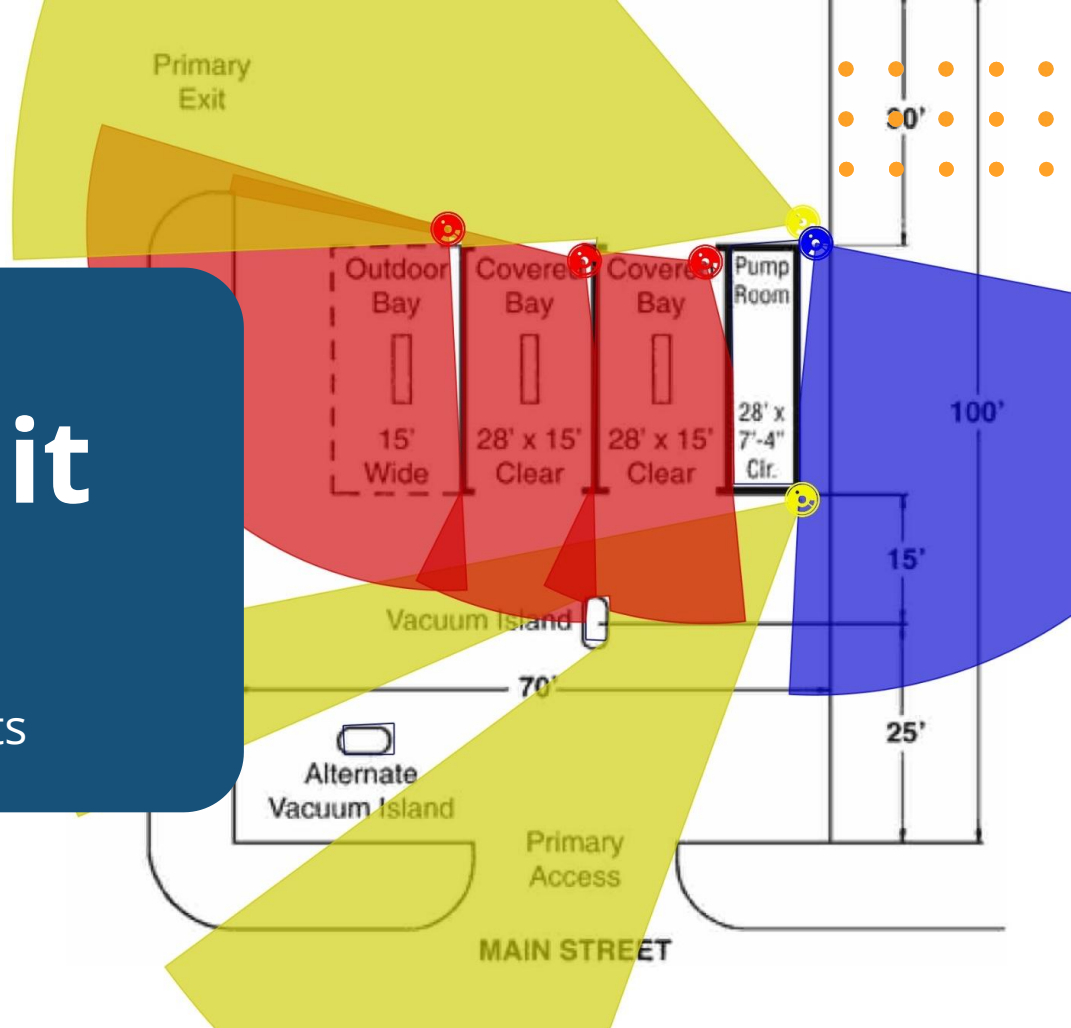
To stay protected in 2026 and beyond, businesses need security that is:

- Proactive (AI driven detection + remote guarding)
- Integrated (video + access + intrusion + cloud management)
- Efficient (more coverage per device, fewer labor hours)
- Documented (audit logs, video evidence, access reports)
- Compliant & future-ready (NDAA, cybersecurity, evolving response requirements)
- In 2026, budget constraints (not technology) will define security decisions.



Security Audit Checklist

Identifying Gaps and Weak Points



Security Audit Checklist



This step-by-step Security Audit Checklist helps you:

1. Find gaps in your physical, technological, and cybersecurity systems.
2. Assess the health and effectiveness of your current security setup.
3. Take action to ensure everything is functioning as it should.

This step by step checklist will help you identify potential vulnerabilities in your system and take corrective action to mitigate risks.

Want to audit your security system with an expert? [Book a call here >](#)

Security Audit

System Health Check

The goal of this audit is to ensure you are following best practices to keep your institution secure.

Checklist



[Download The Sheet Template >](#)

*Make a copy of the sheet template to help store your security audit for long term reference.



Check your Hard Drive / Storage Space

- Does Your NVR (network video recorder) have sufficient space?
- If you need to free up storage space, delete the oldest footage first or consider upgrading your [hard drive](#).



Make Sure you Devices Are Online

- Ensure each camera on your network is on and recording



Make Sure your Lenses Are Cleaned

- Clean your camera lenses with a microfiber cloth and distilled water for the best results.
- Clean lenses will really help improve surveillance footage at night

Technology Audit (Any System)

The goal here is to ensure the VERY basics of cyber security are covered.

Checklist



[Download The Sheet Template >](#)

*Make a copy of the sheet template to help store your security audit for long term reference.



Time to Rotate Your Passwords

- The general rule of thumb is to rotate passwords every 90 days - If you haven't updated your default password - You are long overdue.



Check For Outdated User Accounts

- Check your user permissions and ensure it's up to date. Remove any old staff or applications that are no longer used.



Ensure New Hires Are Onboarded & Trained

- Are there new staff that need access and training? Be sure you schedule this.



Update Firmware

- Are there new staff that need access and training? Be sure you schedule this.

Technology Audit (Surveillance Hardware)

The goal here is to ensure that your hardware is correctly operating.

Checklist



[Download The Sheet Template >](#)

*Make a copy of the sheet template to help store your security audit for long term reference.



Day and Night Footage Quality Check

- Look back at footage from midday and midnight to ensure footage quality is sufficient.



Are all Cameras Online and Recording?

- Are all your cameras on and working correctly? Review system logs for dropped cameras or loss of footage.



Ensure Camera Names are Accurate

- Every user should be able to tell exactly which camera is which just by the name

Security Audit

Technology Audit (Access Hardware)

The goal here is to ensure that your hardware is correctly operating.

Checklist



Visual Inspection

- Check for any frayed wires, rusting components, cracked or scratched screens, dust build up on sensors or card readers



Clean Devices & Components

- Dust and debris can accumulate over time and cause mechanical complications that will ruin your system. Be sure to use anti-corrosion solutions to prevent deterioration. A good cleaning can also reveal any problems hidden beneath dust layers.



Test Sensors

- Perform walk tests with the aim of activating the sensors and verifying proper functionality. Check all readers and push to exit buttons operate correctly



Check All Door Retainers

- Check to ensure door retainers are secure and closers close properly and all the way. (No binding)



Power Checks

- Power checks include examining all wired connections between your main power supply and your security system to ensure they are tight and secure. Check all power supplies that charging voltages are correct.
- You should do the same for connections between the battery backup and the access control system. Then turn the main power supply off and check whether the system transitions smoothly to the battery.



Check Data Logs

- During your maintenance checkups, make sure you go through the data logs in detail to ascertain that no entries show anomalies like incorrect times, etc.

Security Audit

Audit For Any Blind Spots

The goal here is to identify areas of a premises that may be prone to undetected activity or otherwise vulnerable to the activities of malicious actors.

Checklist



Ensure All Entrances Are Covered

- Draw a physical diagram on site indicating where each camera is located and how far its field-of-view extends.



Ensure Bottom Story Windows Are Covered

- Walk around your premises and ensure that bottom story windows have coverage.



Think Like An Intruder

- Ensure all entrances Are covered, but remember not all entrances are doors. Windows at ground level are also potential points of entry.



Think like an insurance adjuster:

- Are there parts of your facility where someone could get hurt? You can lower your liability by making sure that you can continuously observe and record that your building was clean, free of any hazards and that your people are following safety regulations



Think like HR:

- If you didn't document it, it didn't happen. Anywhere employees interact should be recorded, so that there's a document trail should an employee act out

Security Audit

Door Security Audit

Your first and most important security dollar should be spent on secure windows and great doors with good locking mechanisms.

Checklist



For Institutions: Metal doors with Maglocks & Access Control

- We recommend metal doors, maglocks, and an access control / key management system, with an audit report. Handing out physical keys for companies/entities that have transient / semi-trusted individuals who need temporary (think cleaners) or semi-permanent (think employees) access isn't a great plan.



For Homeowners: Good deadbolt and a solid wood door

- We suggest you deal with doors BEFORE investing in a security system

Security Audit

Security Lighting Audit

Night vision is fine for alerting, but if you want to take legal action, color video with natural, white light is going to be easier for the jury to convict.

Checklist



Make sure all exterior lighting continues to work

- Walk the premises to ensure no lightbulbs are burned out or broken



Make sure that all exterior assets or points of entry have adequate lighting

- Did you add any items of value to our outdoor space (a new AC unit, a new vehicle) or change the location of an existing asset?
Make sure you have lighting where you have valuables!

Don't have time to maintain your security system?

Maintaining a surveillance system can be difficult and time consuming. Without a regular maintenance plan, your surveillance system is at risk for breaking down or becoming outdated.

Proactively monitor your systems, minimize downtime and reduce the impact of preventable issues with the SCW service plan.

The SCW team will complete a comprehensive review of your entire Surveillance System to ensure proper working order and preemptively identify any issues with system operation.



[Get The Service Plan >](#)

Get in touch today:

Phone: [828-373-8218](tel:828-373-8218)

Email: hello@getscw.com

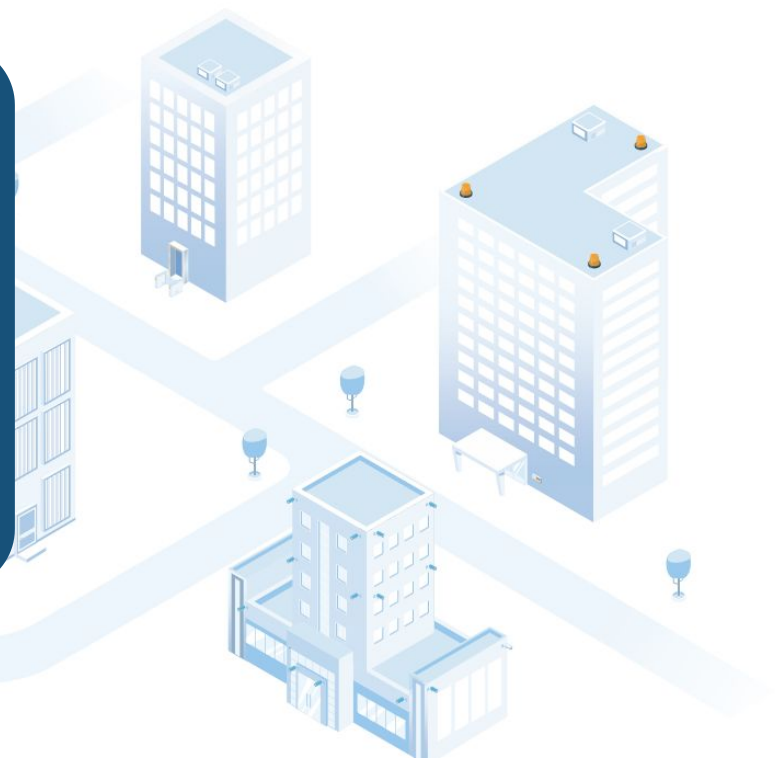
Website: www.getscw.com





Smart Security Budgeting for 2026

Building a Layered Security Approach



Budget Prioritization

Smart Security Budgeting for 2026



What's Included in This Section?

1. Secure Your Perimeter First
2. Detect Intrusions Early
3. Document Everything with Cameras
4. Don't Forget Digital Security

Building an effective security system starts with prioritization. **Layered security** focuses on addressing threats step-by-step, ensuring each layer builds on the previous one for maximum protection.

The Power of Layered Security

- Keep threats out
- Detect breaches quickly
- Document events for action and protection
- Safeguard your digital systems

Budget Prioritization

Secure Your Perimeter First

Your **highest value and most-bang-for-your-buck** should be spent on your **entrances**. Start with the basics: doors, windows, and access control.

- Reinforce entrances with secure locks and durable doors.
- For businesses, upgrade to metal doors and smart access control systems.
 - Reduce rekeying costs with keycards, fobs, or mobile credentials.
 - Monitor for forced entry or doors left open.
- Why it matters: A strong perimeter stops most threats before they escalate.



Budget Prioritization

Detect Intrusions Early

The next layer of security you should invest in is an intrusion detection system. A perimeter breach is taken seriously by police, while suspicious activity and even minor crimes outside are frequently ignored.

A good intrusion system is usually site specific, but here's some consideration that should be taken into account, depending on what building / asset you are trying to secure.

Video Monitoring: For outdoor assets, multi-tenant buildings, or 24/7 operations.

- Essential for locations with open perimeters like construction sites or parking lots.

Key Insight: Intrusion systems tell you when a threat is real and requires action.

Budget Prioritization

Document Everything with Cameras

Use cameras to document:

1. Security breaches
2. Liability issues (false injury claims, HR disputes)
3. Operational performance (safety compliance, productivity monitoring)

Strategically place cameras after defining your access and intrusion systems.

- Focus on entrances, blind spots, and high-value areas.

Why it's critical: Many police jurisdictions now require visual verification before dispatching officers.

Budget Prioritization

Don't Forget Digital Security

We would be doing our clients a disservice if all we ever talked about was protecting your business or other entity from physical threats only. Commercial grade security isn't complete without protecting your organization from digital threats from phishing, to malware, to cyber hijacking, to ransomware.

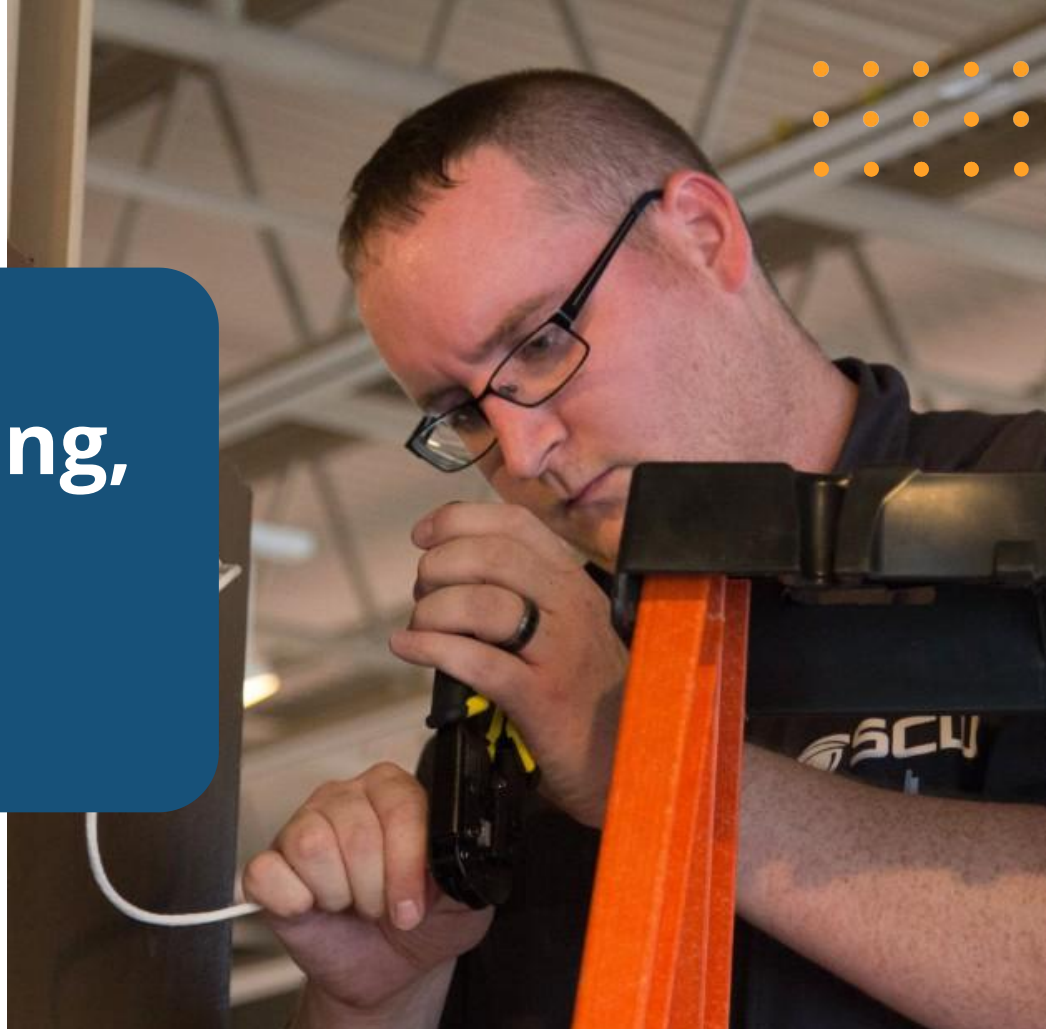
Cyber crime is booming and criminals are targeting smaller entities who are less likely to be prepared.

Modern security must address cyber threats as well as physical ones.

- Protect digital entry points like NVRs, access control systems, and business networks:
 - Regular password rotations and firmware updates.
 - Remove outdated users and monitor for unauthorized access.
- Implement safeguards for data backup, recovery, and ransomware protection.



Ongoing Monitoring, Maintenance, & Optimization



Proactive Management

Monitoring, Maintenance, & Optimization



A security system is only as strong as its upkeep.

Regular maintenance and proactive monitoring ensure your systems stay reliable, efficient, and ready to protect.

What's Included in This Section?

1. Routine Maintenance
2. Monitoring Services
3. Incident Response Planning

Proactive Management

Routine Maintenance

Schedule regular hardware checks:

- **NVR storage:** Ensure you have sufficient recording space.
- **Camera status:** Confirm all cameras are online and functional.
- **Door sensors:** Inspect for proper operation.

Update firmware to enhance performance and safeguard against cyber threats.



Proactive Management Monitoring Services

Professional Monitoring:

- **Remote Guarding:** Proactively respond to incidents in real time with SCW agents. [Learn more >](#)
- **Remote Guarding Cost Calculator:** See how much you can save by switching to real-time, AI-assisted remote guarding. [Learn more >](#)

Self-Monitoring:

- Centralized VMS for real-time notifications and quick action. [Learn more about SCW's VMS >](#)

FASTER, INFORMED, REAL-TIME RESPONSE



DETECT

AI enhanced cameras detect people and vehicles in the area.



ANALYZE

Professional, US based remote guards monitor activity and determine if it's a security threat.



RESPOND

Remote guards respond in a way that fits your unique security challenges.

- Dispatching Police - Live talk down warnings via loud speaker.
- Dispatching on premise guards - all of the above and more.



Proactive Management

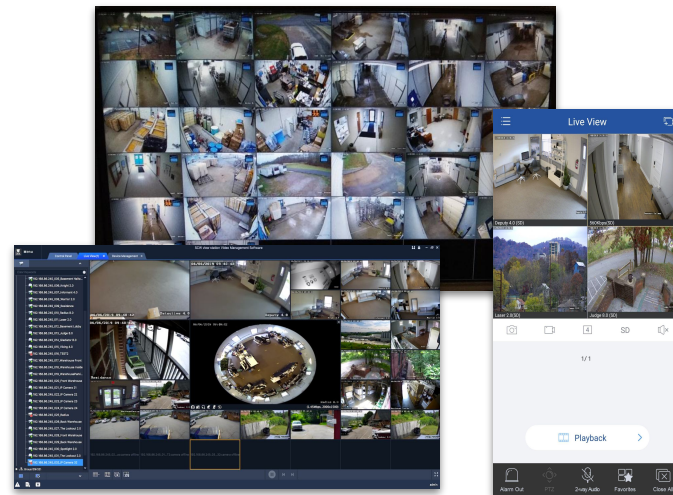
Incident Response Planning

Develop a Clear Protocol:

- Define who to contact and when for security breaches.
- Establish escalation steps for different threat levels.

Post-Incident Reviews:

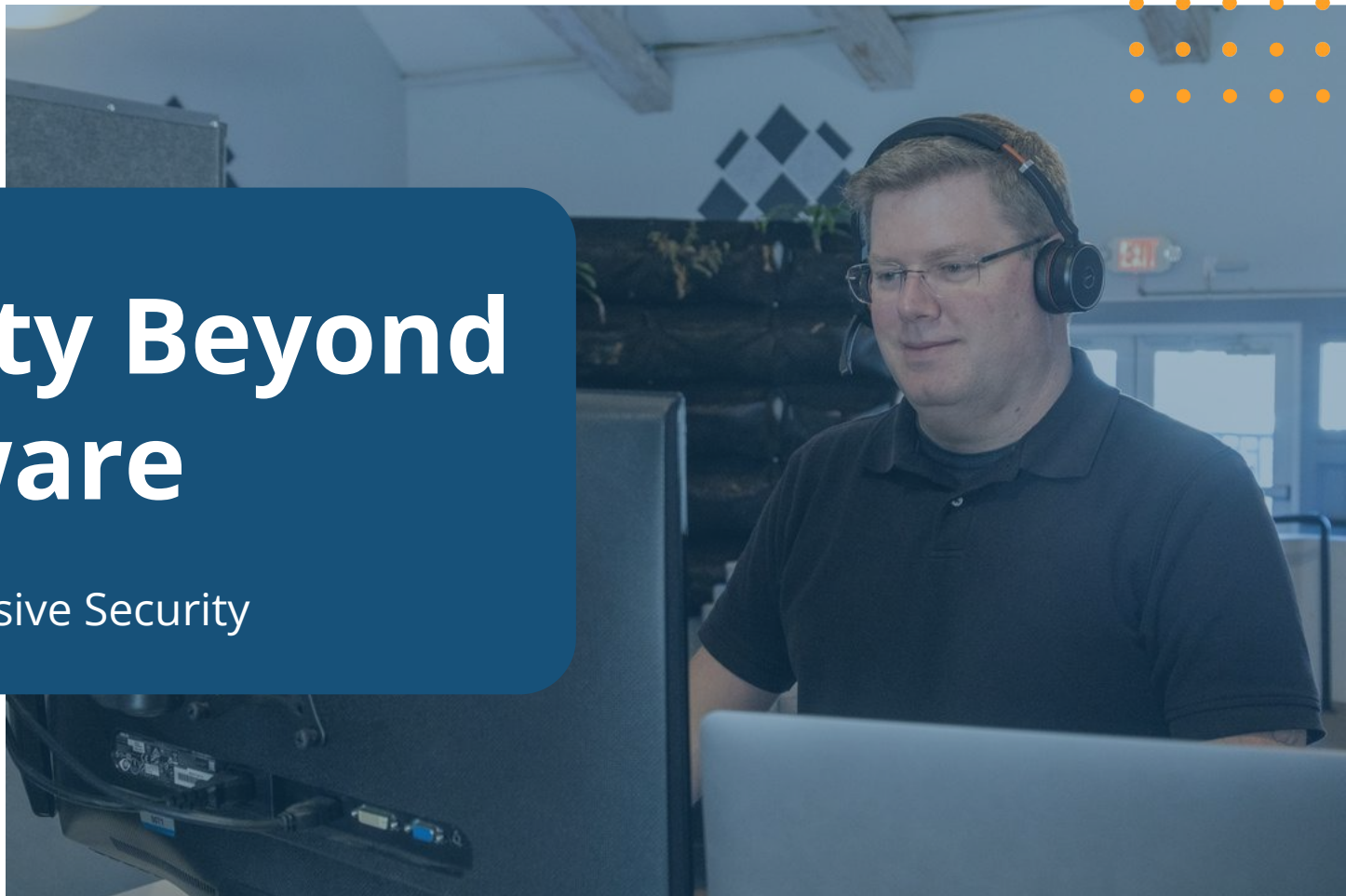
- Analyze incidents to identify weaknesses.
- Optimize systems and strategies to prevent future issues.





Security Beyond Hardware

Go Beyond Passive Security



Security Beyond Hardware

Services That Keep Your Security Strong



A robust security system is only as effective as the support behind it. SCW's professional services go beyond hardware to ensure your investment is:

- Monitored to prevent incidents in real-time.
- Maintained to minimize downtime.
- Optimized for long-term performance.

Why It Matters:

Proactive services maximize uptime, prevent issues, and save you time.

Security Beyond Hardware

Camera Monitoring In Action

Example of a real incident

Here is an example of a real incident:

- **1:45 am**, an unauthorized vehicle drove onto a large construction site. The agents in the Operations Center received an alarm indicating a trespasser.
- **1:47 am**, Intruders are warned through a series of talk-downs, warning intruders to leave the premises immediately. The team initiates client standard operating procedures and contacts appropriate point of contacts (previously specified by the client)
- **1:50 am**, Local police are dispatched to the scene
- **2:04 am**, The intruder is seen leaving the property with stolen property
- **2:16 am**, police arrive on the scene and our agents brief officers on the incident. Leading to the capture of the trespasser and recovery of all stolen property.



Stop incidents before they escalate with Professional Camera Monitoring

As businesses face increasing security challenges, proactive monitoring has become more important than ever.

Unlike traditional camera setups that only record footage, remote guarding enables real-time intervention.

Trained operators can engage with intruders based on your standard operating procedure.



**Get Professional Camera
Monitoring >**

Get in touch today:

Phone: 828-373-8218

Email: hello@getscw.com

Website: www.getscw.com



Security Beyond Hardware

Surveillance System Service Plan

Proactive Maintenance to Protect Your Investment

Minimize downtime that costs you critical footage, keep your system performing like new. Focus on your business while SCW keeps you secure.

System Health Checks:

- Verify NVR settings, storage, and firmware updates.
- Ensure all cameras are online, named, and delivering high-quality footage (day & night).
- Complete a S.M.A.R.T. test for hard drive health.

Preventative Maintenance:

- Adjust views, clean equipment, and troubleshoot issues.
- On-site service for issues that can't be fixed remotely.
- Same-day or next-day service priority available.

Configuration Backups:

- Snapshots of system settings for quick recovery.



Protect Your Investment with an SCW Service Plan

Maintaining a surveillance system can be difficult and time consuming. Without a regular maintenance plan, your surveillance system is at risk for breaking down or becoming outdated.

Proactively monitor your systems, minimize downtime and reduce the impact of preventable issues with the SCW service plan.

The SCW team will complete a comprehensive review of your entire Surveillance System to ensure proper working order and preemptively identify any issues with system operation.



[Get a Service Plan >](#)

Get in touch today:

Phone: [828-373-8218](tel:828-373-8218)

Email: hello@getscw.com

Website: www.getscw.com



Security Beyond Hardware

Commercial Security Installation Services

Get It Done Right with SCW Experts

Avoid costly mistakes with professional setup, save time and resources.
Flexible for single-site businesses or complex multi-location setups

End-to-End Installation:

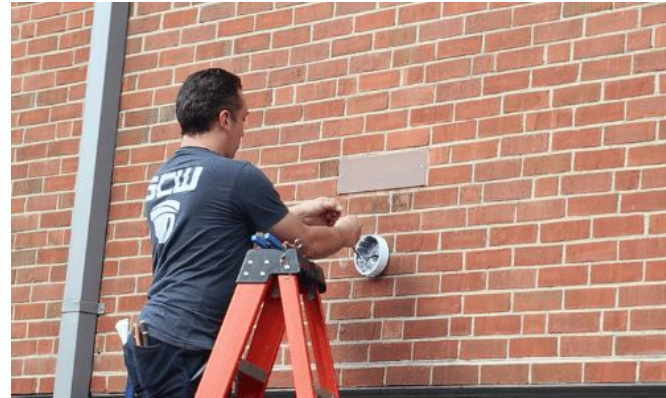
- Cables, cameras and access control – professionally installed.
- Custom configuration of NVRs and system settings.

Tailored Design:

- Solutions built for your site's needs – eliminate blind spots, secure critical areas.
- Scalable for future growth.

Post-Installation Support:

- Hands-on training for your team.
- Lifetime technical support from SCW.



Save time and resources with Professional Installation

We'll deliver your systems then get them up and running.

We'll configure your systems and train you on how to use them.

Unlike most installers, support is included. Get answers to your questions with free technical support for life.



[Professional Installation >](#)

Get in touch today:

Phone: [828-373-8218](tel:828-373-8218)

Email: hello@getscw.com

Website: www.getscw.com



Ready to Secure Your Organization for 2026?

Don't leave your organization's safety to chance.

Schedule a free security review with SCW today to:

- **Assess Your Current Security Setup:** Identify gaps and vulnerabilities with expert insights.
- **Receive a Customized Plan:** Get tailored recommendations and a free floor plan design
- **Protect Your Investment:** Ensure your systems are optimized, monitored, and ready for what's next.

Rated
4.9/5

Across 3,272 reviews

15,000

Customers Served

255k

Installed Cameras



Schedule Your 2026 Security Plan

Start the year with confidence by scheduling a free security review with SCW.

[Book a Security Review >](#)