

WYZE Security Assessment Tool

Immediate Action Plan for Multi-Location Implementation

For: Multi-location business operations requiring enterprise-grade security **Goal:** Achieve 10/10 security mastery in 30 days

IMMEDIATE ASSESSMENT (Complete First)

Current State Questionnaire

Answer each question to determine your starting point:

1. Account Security (Current Score: ____/8)

- Is your WYZE password unique and 16+ characters? (0=No, 2=Yes)
- Do you have 2-factor authentication enabled? (0=No, 2=Yes)
- Do you use a password manager? (0=No, 2=Yes)
- Have you shared account access with others? (2=No/Documented, 0=Yes/Undocumented)

2. Network Setup (Current Score: ____/10)

- Are cameras on a separate network from business devices? (0=No, 4=Yes)
- Have you changed default router passwords? (0=No, 2=Yes)
- Is WPA3/WPA2 enabled with strong encryption? (0=No, 2=Yes)
- Do you monitor network traffic? (0=No, 2=Yes)

3. Device Management (Current Score: ____/10)

- Are all cameras on latest firmware? (0=No, 3=Yes)
- Have you changed default device names? (0=No, 2=Yes)
- Are detection zones properly configured? (0=No, 3=Yes)
- Do you have local backup recording? (0=No, 2=Yes)

4. Location Coverage (Current Score: ____/7)

- Do you have cameras covering all entry points? (0=No, 2=Yes)
- Are critical areas under 24/7 surveillance? (0=No, 2=Yes)
- Do you have redundant coverage for high-value areas? (0=No, 2=Yes)
- Is storage capacity adequate for retention needs? (0=No, 1=Yes)

30-DAY MASTERY PLAN

WEEK 1: SECURITY FOUNDATION

Days 1-2: Account & Access Hardening

- ☐ Generate new 20-character password using password manager
- ☐ Enable 2FA with authenticator app (not SMS)
- ☐ Document all authorized users and access levels
- ☐ Set up shared access properly (if needed for business)

Days 3-4: Network Isolation

- ☐ Create dedicated IoT network: "BusinessSec_[Location]"
- ☐ Move all WYZE devices to isolated network
- ☐ Configure firewall rules blocking IoT-to-main network access
- ☐ Test connectivity and streaming quality

Days 5-7: Device Inventory & Updates

- ☐ Complete comprehensive device audit (use provided template)
- ☐ Update all devices to latest firmware
- ☐ Rename all cameras with location-specific names
- ☐ Document MAC addresses and IP assignments

WEEK 2: OPTIMAL CONFIGURATION

Days 8-10: Camera Optimization

- ☐ Configure detection zones for each camera
- ☐ Set up person/vehicle detection appropriately
- ☐ Optimize recording quality vs. bandwidth usage
- ☐ Configure privacy zones where needed

Days 11-12: Storage Implementation

- ☐ Set up local NVR or NAS system
- ☐ Configure RTSP streams (if using advanced recording)
- ☐ Implement automated backup procedures
- ☐ Test recovery from local storage

Days 13-14: Alert System Setup

- ☐ Create tiered alert categories (Critical/High/Medium/Low)

- ☐ Configure multiple notification channels
- ☐ Set up detection schedules (different rules for business hours)
- ☐ Test all alert mechanisms

WEEK 3: DATA PROTECTION & MONITORING

Days 15-17: Backup & Encryption

- ☐ Enable encryption on all storage systems
- ☐ Set up offsite backup for critical locations
- ☐ Configure automated retention policies
- ☐ Document data recovery procedures

Days 18-19: Advanced Monitoring

- ☐ Set up centralized monitoring dashboard
- ☐ Configure bandwidth monitoring
- ☐ Implement system health alerts
- ☐ Create standard operating procedures

Days 20-21: Testing & Validation

- ☐ Conduct backup restoration test
- ☐ Verify all alert paths work correctly
- ☐ Test remote access capabilities
- ☐ Document any issues found

WEEK 4: MULTI-LOCATION & OPTIMIZATION

Days 22-24: Scaling Implementation

- ☐ Standardize configurations across all locations
- ☐ Create deployment templates for new locations
- ☐ Set up location-specific monitoring
- ☐ Implement centralized management tools

Days 25-26: Staff Training

- ☐ Create user training materials
- ☐ Train authorized personnel on system operation
- ☐ Document response procedures for alerts
- ☐ Establish maintenance schedules

Days 27-30: Final Assessment

- ☐ Complete comprehensive security audit

- ☐ Fix any identified vulnerabilities
 - ☐ Update all documentation
 - ☐ Celebrate achieving "Unfuckwithable" status!
-

CRITICAL SUCCESS FACTORS

For Multi-Location Business Operations:

1. Compliance Considerations

- Ensure recording retention meets legal requirements
- Document privacy policies for employee/visitor recording
- Implement access controls meeting business standards
- Regular audit trails for compliance purposes

2. Business Continuity

- Redundant internet connections for critical locations
- UPS backup power for cameras and network equipment
- Alternative access methods if primary systems fail
- Incident response procedures documented

3. Scalability Planning

- Standardized equipment lists for location types
 - Automated deployment procedures
 - Centralized management and monitoring
 - Budget planning for growth and upgrades
-

EMERGENCY RESPONSE PROTOCOLS

If Security Breach Detected:

1. Immediate (0-5 minutes)

- Document the alert with screenshots
- Verify if genuine threat or false positive
- Notify appropriate personnel

2. Short Term (5-30 minutes)

- Review recorded footage

- Coordinate with security/law enforcement if needed
- Secure physical location if necessary

3. Follow-Up (Within 24 hours)

- Complete incident report
 - Review and improve detection settings
 - Update response procedures if needed
-

MAINTENANCE SCHEDULE

Daily:

- Review critical alerts from previous 24 hours
- Check system status dashboard

Weekly:

- Verify all cameras operational
- Review storage capacity
- Test one backup system

Monthly:

- Update firmware if available
- Review and rotate passwords
- Audit user access permissions
- Test complete backup restoration

Quarterly:

- Comprehensive security assessment
 - Update response procedures
 - Staff training refresher
 - Budget review for upgrades
-

SUCCESS METRICS

Technical Metrics:

- 99.9% camera uptime across all locations

- <5% false positive alert rate
- 100% successful backup verifications
- <30 second alert notification time

Business Metrics:

- Zero security incidents due to camera system failures
- Compliance audit passes
- Reduced security-related insurance premiums
- Staff confidence in security systems

Ready to start? Complete the assessment questionnaire above, then begin Week 1 immediately.

Next Step: Send me your assessment scores and I'll create a customized 30-day implementation plan specific to your locations and business needs.