WORKSHEET | 2026 Edition

Security platform evaluation checklist.

As security environments scale, the challenge is no longer just monitoring devices. Security leaders must coordinate infrastructure, vendors, projects, and lifecycle management across multiple locations.

Use this worksheet to evaluate whether a platform can support your operational needs today, and scale with your security infrastructure tomorrow.

siteowl®

HOW TO USE THIS EVALUATION WORKSHEET.

Selecting the right physical security management platform can be challenging. Many vendors offer similar features, but their ability to support real-world security operations can vary significantly.

This worksheet helps security leaders evaluate platforms across five critical capability areas:

Architecture & deployment.	Can the platform support hybrid infrastructure and multi-site environments?
Integration & ecosystem fit.	Does it unify data across video, access control, alarms, and other systems?
Scalability & growth.	Will it support expanding facilities, devices, and teams?
Operational visibility.	Does it provide clear system documentation and infrastructure visibility?
Lifecycle & asset management.	Can it track device health, warranties, and upgrade timelines?

- Mark Yes or No based on vendor capabilities.
- Use the Notes section to record limitations or implementation details.
- Score each vendor in the comparison worksheet to identify the best fit.

By the end of the evaluation, you'll have a clear side-by-side comparison of the platforms best suited for your security environment.

SECTION 1: ARCHITECTURE & DEPLOYMENT.

Modern physical security platforms must support multi-site operations, remote management, and hybrid infrastructure environments. Many legacy systems were designed for a single facility and struggle to support today's distributed security programs. Use this section to evaluate whether the platform architecture can scale with your organization.

• Supports hybrid cloud deployment.	Yes	No
• Centralized multi-site management.	Yes	No
• Vendor-neutral hardware support.	Yes	No
• Remote administration capability.	Yes	No
• Scalable infrastructure.	Yes	No

Notes: _____

SECTION 2: INTEGRATION & ECOSYSTEM FIT.

Security platforms deliver the most value when they connect systems and unify data across the security environment. The best platforms do more than connect to video, access control, and alarm systems. They create a single operational view across technologies, allowing security teams, IT, and vendors to work from the same information.

- Integrates with video systems. Yes No
- Integrates with access control. Yes No
- Integrates with alarm systems. Yes No
- Creates unified system data. Yes No
- Supports open APIs / integrations. Yes No

Notes: _____

SECTION 3: SCALABILITY & GROWTH.

As organizations expand, security teams must manage more facilities, more devices, and more vendors. True scalability is not just about device count. It also means maintaining accurate documentation, consistent configurations, and operational visibility as systems evolve. Use this section to assess whether the platform can support long-term growth.

- Fast on boarding of new sites. Yes No
- Maintains accurate as-built documentation. Yes No
- Centralized configuration updates. Yes No
- Scalable user permissions. Yes No
- Operational efficiency at scale. Yes No

Notes: _____

SECTION 4: OPERATIONAL VISIBILITY.

Across many organizations, security system information is scattered across spreadsheets, CAD drawings, installation photos, and vendor documentation. Modern platforms replace this fragmented approach with living system documentation and visual infrastructure mapping. Use this section to evaluate whether the platform provides clear operational visibility into your environment.

- Digital floorplans & device maps. Yes No
- Living system documentation. Yes No
- Device configuration tracking. Yes No
- Installation-to-operations workflow. Yes No
- Vendor access to system data. Yes No

Notes: _____

SECTION 5: LIFECYCLE & ASSET MANAGEMENT.

Every security device has a lifecycle, from installation to maintenance to eventual replacement. Without centralized visibility into device age, service history, and warranty status, security teams are often forced into reactive maintenance and unplanned upgrades. Evaluate whether the platform supports proactive lifecycle planning.

- Tracks device age and lifecycle. Yes No
- Tracks warranties & contracts. Yes No
- Tracks maintenance history. Yes No
- Supports proactive upgrades. Yes No
- Supports capital planning. Yes No

Notes: _____

VENDOR COMPARISON WORKSHEET.

Score each vendor 1–5 per category.

VENDOR NAME: _____

• Architecture & deployment.	1	2	3	4	5
• Integration & ecosystem fit.	1	2	3	4	5
• Scalability & growth.	1	2	3	4	5
• Operational visibility.	1	2	3	4	5
• Lifecycle & asset management.	1	2	3	4	5

Notes: _____

OVERALL SCORE.

Sum of all category scores: Max 25 _____ **/ 25**

Scoring guide:

1	Does not meet requirement.
2	Partially meets requirement.
3	Meets minimum requirement.
4	Exceeds requirement.
5	Fully exceeds (best in class).

About SiteOwl

SiteOwl is the only physical security system lifecycle management platform that brings enterprise security teams, their security vendors, and assets together on one unified platform.

The solution's suite of applications connect real-time data and workflows, specific to the physical security industry, to drive collaboration, visibility and efficiency.

To learn more, please visit getsiteowl.com.