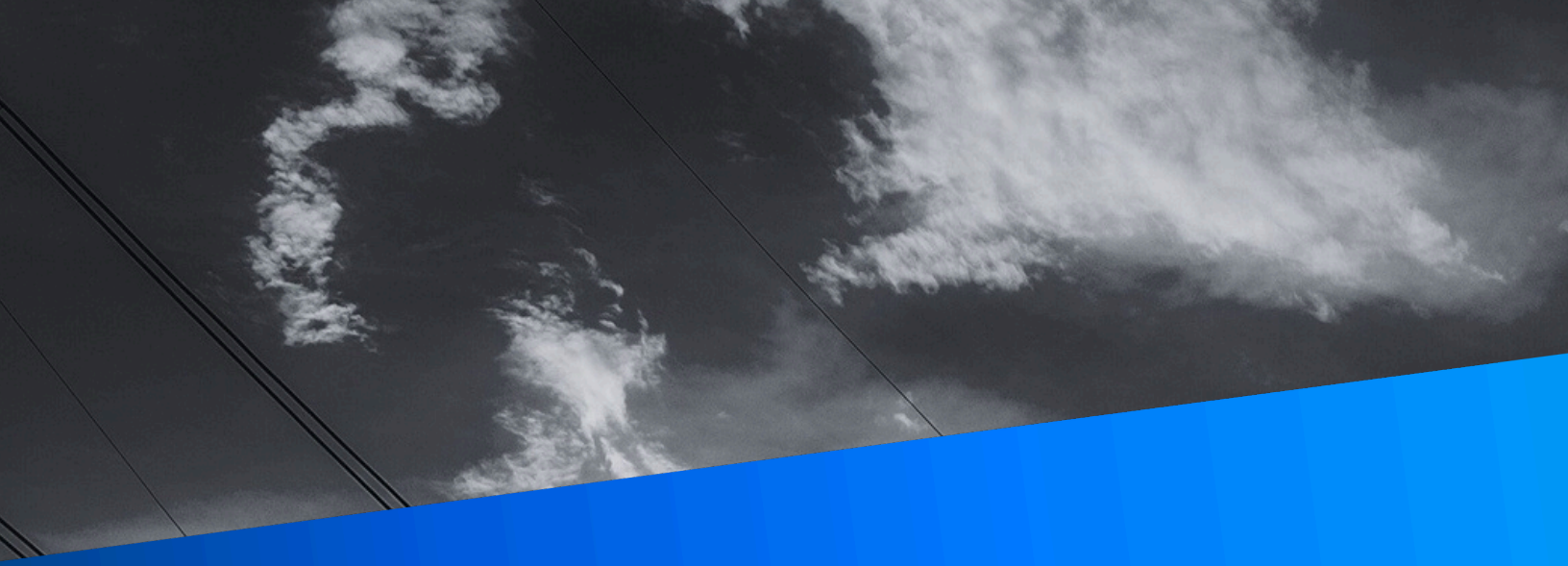


UTILITIES AND ENERGY

Physical Security Infrastructure Management

Cutting-edge strategies and proven techniques to elevate security in Utility and Energy Sectors

siteowl®

Table of contents

INTRODUCTION

Safeguarding infrastructure in the utilities and energy sectors is no walk in the park. It's a high-stakes, high-pressure job that involves overseeing a vast number of security assets across numerous distant sites. With the constant threat of security breaches and the absolute necessity of these infrastructures, it's crucial for big businesses in this sector to bank on technology that not only bolsters their security measures but also simplifies the management of these security systems.

There are a number of unique challenges in protecting utilities and energy infrastructure.

- **Critical infrastructure protection**
  Power plants, substations, and pipelines are prime targets for physical and cyber attacks, with the potential for devastating consequences.
- **Remote asset security**
  Many facilities are located in isolated areas, making them vulnerable to theft, vandalism, and unauthorized access.
- **Environmental threats**
  Extreme weather, natural disasters, and wildlife pose significant risks to infrastructure and operations.

These challenges, coupled with operational complexities like aging infrastructure, vendor coordination, and the need to balance maintenance with innovation, demand a comprehensive and adaptable security strategy.

1,700

physical security incidents were reported to the E-ISAC in 2022, an increase of 10.5% from 2021, according to the North American Electric Reliability Corporation (NERC)'s Electricity Information Sharing and Analysis Center (E-ISAC).

SECURELY NAVIGATING THE FUTURE

Utilities, our modern life's backbone, are essential services providing us with electricity, water, and gas. However, this industry is increasingly under threat from physical security attacks. It's no secret that our electric infrastructure faces security threats, like copper theft, on a regular basis. Yet, more complex threats have recently begun to surface. The energy sector, in particular, is seeing a rise in incidents, with substations, transformers, and power lines increasingly becoming targets.

Keeping pace with the changing landscape

In March 2024, a Tesla factory in Germany was plunged into darkness due to an act of arson on a nearby electricity pylon. This left the factory and the surrounding areas powerless, inflicting hefty losses on Tesla running into hundreds of millions. But what led to this situation where arsonists could cause such disruption?

The answer probably lies in the outdated methods utilities and energy companies still employ to manage their security infrastructure.

In the U.S. alone, there are over 55,000 substations, 200,000 miles of transmission lines, and 6 million miles of distribution lines, according to statistics from the Department of Energy Office of Electricity. Many of these grid assets are located in remote areas where assigning a security guard to each asset isn't always practical. It begs the question: How do we equip security teams at utilities and energy companies to manage their infrastructure effectively?

Only

12%

of energy companies are currently using advanced centralized security systems, indicating a significant gap in adopting modern technologies.

Cloud adoption and security convergence

For utility and energy companies, staying ahead of the curve with risk-informed solutions is a game-changer. However, the journey to cloud technology adoption has its fair share of hurdles for these industries. Here are some reasons why:

- Concerns around the safety of sensitive information stored in the cloud.
- Regulations that permit a profit margin on CAPEX, like servers and on-prem equipment, but not on OPEX, like cloud services.
- Reluctance to give up existing on-prem systems.

However, the benefits of the cloud are too valuable to ignore, with more companies starting to adopt cloud based technology.

What does this mean for security teams?

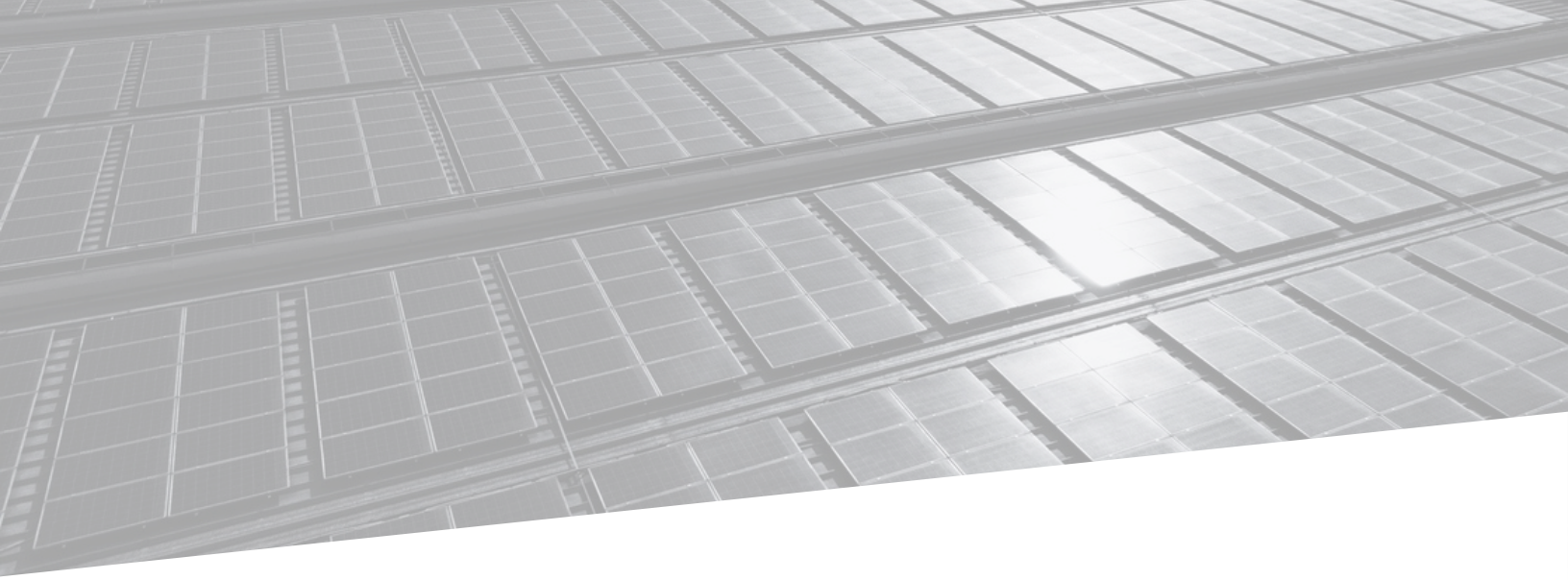
With the shift towards digital infrastructures, security teams in utilities and energy companies increasingly recognize the value of streamlining their security management processes to bolster overall operational efficiency and ensure robust security measures.

One significant hurdle in achieving streamlined operations is the disjointed nature of traditional security management systems. Effective lifecycle management, a key component in ensuring a robust security posture, relies on the ability to make data-driven decisions; something that is hard to accomplish when asset information is stored in one place, warranty information in another, service history in a third and project information in a fourth system.

As we move forward, the rapid advancement of technology in physical security will increasingly take center stage, using smart automation and advanced management to stay ahead. There's no one-size-fits-all solution to physical security, but a good start is to centralize the management of physical security infrastructure.

75%

of organizations observe a reduction in project timelines when using centralized security systems, according to the 2023 TechAdvantage Security Solutions report.



SIMPLIFYING PHYSICAL SECURITY INFRASTRUCTURE MANAGEMENT

The protection of critical infrastructure is no small task. It takes a variety of techniques and strategies to shield these crucial systems from harm. But when the very devices that are essential to ensuring a strong security posture are managed using antiquated methods like paper floor plans and spreadsheets, it's hard to not acknowledge there's a problem.

Ask any security leader about how their team handles security projects and asset management, you'll hear a range of responses from "We use spreadsheets to track warranty information" or "We email our integrator whenever a camera is down" or "We rely on our integrator for updates on how the project is progressing." There's nothing inherently wrong with any of these statements, but the truth is, this is how things have been done for the last two decades.

Crucial information remains scattered, and traditional tools are still in use. When upgrades or retrofits are due, security personnel find themselves scrambling for old CAD drawings and hoping they're still relevant.

Siloed systems lead to redundant workflows, miscommunication among teams, delays in response times and poor planning.

There's no one-size-fits-all solution to physical security, but by centralizing their security management systems, utilities and energy companies not only prepare themselves for current challenges but future-proof their operations against evolving threats.

82%

enterprises report excessive operational delays due to outdated security management systems according to the 2023 Global Security Management Survey.

Managing the lifecycle of physical security infrastructure

Lifecycle management is an often overlooked, but integral, part of physical security. Physical security systems must be constantly monitored and maintained to ensure that they function as intended and provide the level of protection required by an organization.

Physical security lifecycle management is the process of planning, implementing, maintaining, and upgrading physical security measures to protect an organization's assets and personnel. This includes assessing risks, designing security systems, implementing controls, monitoring and testing the systems, and continuously improving the security posture.

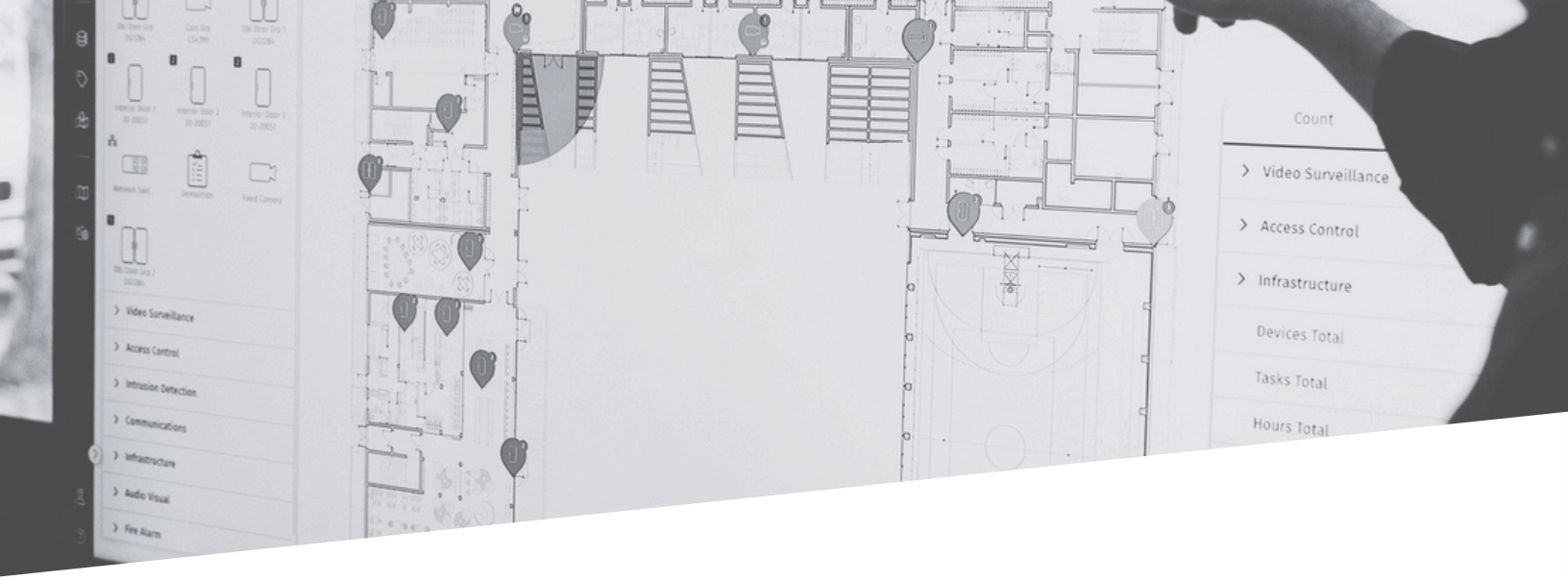
The goal of physical security lifecycle management is to ensure that an organization's physical security measures are effective, efficient, and aligned with the organization's overall security strategy. Some of the challenges impacting both the effectiveness of security systems and the focus of enterprise security teams are:

- **Incomplete system information**
  Not knowing what you have, how old it is, where it is when its warranty expires.
- **Lack of visibility**
  Not knowing how projects are progressing without needed to resort to phone calls and site visits.
- **Inconsistency**
  Not having standardized processes for design, installation, service and audits.

Lifecycle management in the utilities and energy industries provides several benefits. Firstly, it improves the overall security posture by ensuring that security measures are up-to-date and tailored to meet the specific needs of the organization. This helps to save costs as potential security threats can be identified and addressed before they become costly security incidents.

Secondly, it ensures compliance with relevant regulations, standards, and best practices.

Thirdly, it helps to better manage risks associated with physical security by conducting regular risk assessments and addressing potential security threats. Lastly, effective physical security measures and systems enable manufacturing organizations to operate more efficiently by minimizing disruptions and downtime caused by security incidents.



CENTRALIZING INFRASTRUCTURE MANAGEMENT WITH SITEOWL

SiteOwl is a lifecycle management platform purpose-built for enterprise security teams.

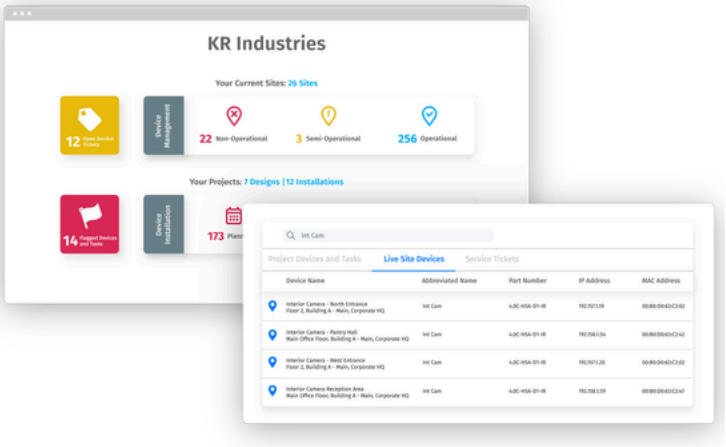
Customers use SiteOwl to create and standardize designs, effectively manage projects, vendors, and manage their security assets, all from a single interface. This provides unparalleled visibility into their security infrastructure, enabling them to budget their security spends effectively and deliver safer environments at a lower cost and with higher confidence.

With SiteOwl, teams can

- **Build faster and better designs** by standardizing the design process and facilitating real-time collaboration with other teams.
- **Achieve on-time and on-budget projectswith real-time installation progress** from vendors in the field.
- **Get faster vendor quotes**by generating accurate project scopes and streamlining the bid process.
- **Improve speed of service resolution**by relaying all necessary information on a digital floorplan.
- **Consolidate all security infrastructure information** across all locations for effective planning and budgeting.

Simplifying project and asset management

SiteOwl simplifies how security teams interact with their systems, other teams and vendors, breaking down the complex and unpredictable into clear and manageable. With a platform that is purpose-built for physical security teams, your security management is both effective and straightforward.

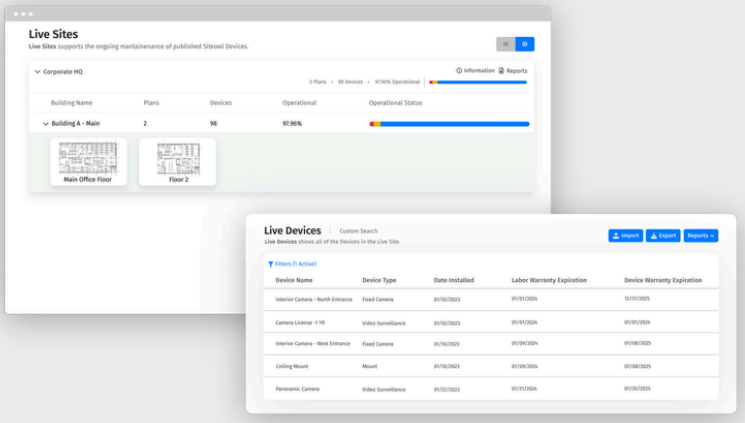


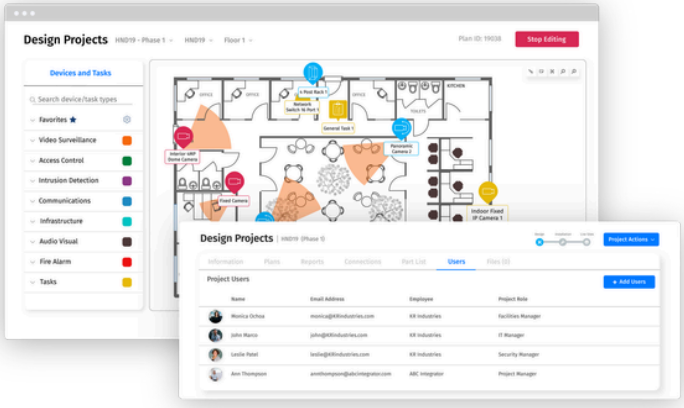
System-wide visibility

No more piecing together fragmented information. With SiteOwl, you get a complete view of your infrastructure, across all your locations.

Always accurate As-builts

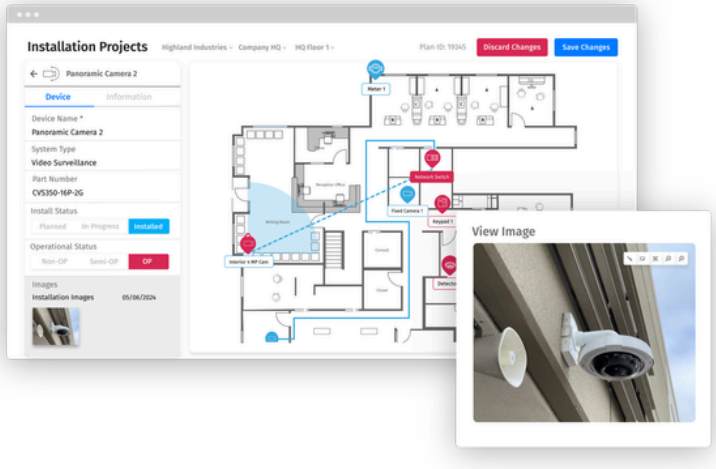
Aggregate your infrastructure changes over time in one central location. SiteOwl gives you and your team the confidence that your information is accurate.





Collaborate across teams

Share updates, track progress, and ensure everyone is marching to the same beat. SiteOwl fosters seamless communication between your internal teams and external vendors.

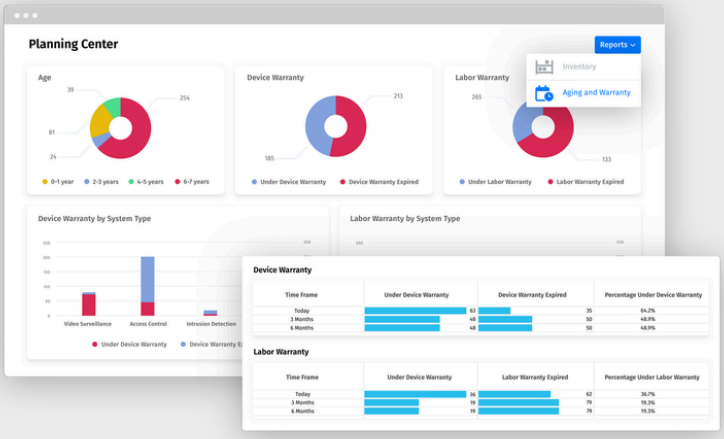


Manage designs and projects

From design to installation, everything is centralized and real-time, ensuring clarity and keeping everyone in the loop.

Effectively plan and budget

Budgeting shouldn't feel like a guessing game. With SiteOwl's analytics, you can make informed decisions based on real data and plan your security investments with confidence.



Tailored for physical security

SiteOwl's suite of apps is tailored for various roles within the physical security ecosystem. Whether you're a technician or a security manager, there's an app for you.

The future of physical security is right now.

Managing security systems shouldn't feel like deciphering a cryptic puzzle. SiteOwl offers security teams a clear vantage point, simplifying security lifecycle management, while improving team efficiency. It's not just a tool, but a comprehensive solution that brings clarity, efficiency, and control to your security infrastructure. With our commitment to world-class support, tailored success strategies, and professional services, we ensure that your transition to SiteOwl is seamless and impactful. That's why high performing security teams across the globe choose SiteOwl.

On average, organizations that use SiteOwl see a 30% reduction in operational costs and a 40% improvement in response times, all while ensuring the resilience and reliability of critical infrastructure in an increasingly complex security landscape.

For more information about SiteOwl, visit www.getsiteowl.com or request a demo.