eBook

everbridge™

# 15 questions to ask vendors

PSIM software buyer's guide

# Introduction

In an era where both the complexity and volume of security threats continue to increase, organizations across the spectrum—be it in the public sector, private sector, or governmental bodies—must prioritize the management and integration of their security systems.

This is where Physical Security Information Management (PSIM) software becomes crucial. As security challenges become more multifaceted and frequent, PSIM has emerged as a popular choice for organizations seeking a holistic and integrated approach to security management. PSIM software is designed to offer an integrated and comprehensive view of security operations, enhancing situational awareness and improving response coordination. Choosing the right PSIM vendor is therefore not just about purchasing software, but investing in a system that can evolve with your security needs.

If you are confident about the value of PSIM for your organization, these questions will guide you in selecting the right vendor. If you're still unsure, consider taking our "Is PSIM right for you? Quick assessment" to evaluate your organization's needs and the potential benefits of implementing a PSIM system.

**Here are the 15 most critical questions to ask prospective PSIM vendors before making your decision.**

## 1. How does the PSIM software integrate with existing security systems?

Understanding how the PSIM solution will work with your current security infrastructure is essential. Ask if the software supports integration with various types of hardware and systems such as CCTV, access control, intrusion detection, and fire alarms. Verify if it supports open standards for interoperability.

## 2. Can the system scale to meet future needs?

Your organization may grow or face new security challenges over time. Ensure the PSIM solution can scale in terms of additional users, devices, and geographic locations. Ask about the vendor's track record in supporting scalable implementations.

## 3. What is the system's capability in terms of real-time data processing and situational awareness?

Real-time data processing is crucial for effective situational awareness. Ask how the system processes and displays data from various sources in real-time. Check if it provides a unified interface for viewing all data streams.

## 4. Does the system support mobile access and remote operations?

Security personnel need to access the system from various locations. Ask if the PSIM software offers mobile applications or web-based interfaces that allow remote access to live data, alerts, and system controls.

## 5. What are the system's incident management and response capabilities?

Effective incident management is a core function of PSIM systems. Inquire about the software's capabilities in terms of incident detection, classification, response coordination, and post-incident analysis. Check if it supports automated workflows and alerts.

## 6. How does the system handle data security and compliance?

Security of the data processed by the PSIM system is critical. Ask about the system's data encryption methods, user authentication processes, and compliance with relevant security standards and regulations (e.g. GDPR, ISO 27001).

## 7. Can the system provide comprehensive reporting and analytics?

Detailed reporting and analytics are essential for assessing the effectiveness of your security operations. Ask if the system can generate custom reports and provide analytics on incidents, response times, and system performance.

## 8. Is the user interface intuitive and user-friendly?

A complex system can hinder the effectiveness of your security team. Ask for a demonstration to assess the user interface's intuitiveness and ease of use. Ensure it can be operated efficiently under stress.

## 9. Does the vendor offer robust support and training?

The quality of support and training provided by the vendor can significantly impact the success of the implementation. Ask about the availability of customer support, training programs, and resources for ongoing education.

## 10. What are the customization options available?

Every organization has unique requirements. Ask about the level of customization available within the PSIM software, including custom workflows, dashboards, and reporting tools to tailor the system to your specific needs.

## 11. How does the system ensure high availability and reliability?

The PSIM system must be reliable and available during critical events. Ask about the vendor's uptime guarantees, disaster recovery processes, and redundant systems to ensure continuous operation.

## 12. What are the integration capabilities with other business systems?

A comprehensive security management approach may require integration with other business systems like HR databases, building management systems, and ERP solutions. Ask if the PSIM software can seamlessly integrate with these systems.

## 13. Can the system be configured for different user roles and permissions?

Role-based access control is important for managing who can access and manipulate different parts of the system. Ask if the PSIM software allows for granular role definitions and permissions settings.

## 14. Does the system support video analytics and advanced monitoring technologies?

Advanced video analytics can enhance security operations by providing automated detection and alerts. Ask if the PSIM software supports integrating video analytics and how it handles data from such technologies.

## 15. What is the total cost of ownership (TCO)?

Understanding the total cost of ownership, including initial licensing, implementation, maintenance, and future upgrades, is critical. Ask for a detailed breakdown of all costs associated with the PSIM solution to avoid hidden expenses.

# Conclusion

Choosing the right PSIM vendor is crucial for the safety and security of your organization. By asking these 15 questions, you can ensure the solution aligns with your operational requirements, offers scalability for future needs, and provides robust security and compliance features. A well-selected PSIM system will enhance situational awareness, streamline incident management, and ultimately safeguard your organization's assets and people.

Everbridge has been a leader in security technology for over twenty years, providing comprehensive solutions for critical event management. Taking the next step towards a comprehensive security management system with Everbridge Control Center could be pivotal in enhancing your organization's security posture. We invite you to schedule a demo to see firsthand how our solution can meet your needs and help you manage your security operations more effectively.

## Request a demo of Everbridge Control Center

By leveraging the advanced features and integration capabilities of Everbridge Control Center, you can ensure your organization remains secure, responsive, and ahead of potential threats.

Go to https://www.everbridge.com/demo/

everbridge™

# About Everbridge

Everbridge, Inc. empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

Visit Everbridge.com

Read our company blog

Follow us on LinkedIn

Follow us on Twitter

Get in touch to learn about Everbridge, empowering resilience.

everbridge™