GIGAOM

COMMISSIONED BY:

graylog

Navigating the SIEM Market Transition

SECURITY & RISK


GIGA
OM

GigaOm CxO Decision Brief: Navigating the SIEM Market Transition

Solution Value

Graylog provides a flexible SIEM solution designed for mid-to-large enterprises. By prioritizing simplicity and scalability, it offers streamlined threat detection and response, reducing the complexity of traditional SIEM systems while supporting diverse cloud environments.

Benefits

Graylog delivers measurable operational and cost advantages to mid-to-large enterprises, enhancing security efficiency while reducing complexity:

- Cost savings through reduced licensing fees and simplified deployments.
- Flexible on-premises, private, or public cloud deployment options.
- Enhanced analyst productivity with intuitive dashboards and streamlined workflows.

Regular platform updates, ensuring effective security without costly overhauls.

Urgency

Immediate consideration is crucial for organizations facing frequent security threats or planning SIEM transitions, refreshes, or updates. It is highly relevant for sectors like finance and healthcare, where compliance and data security are paramount.

Impact

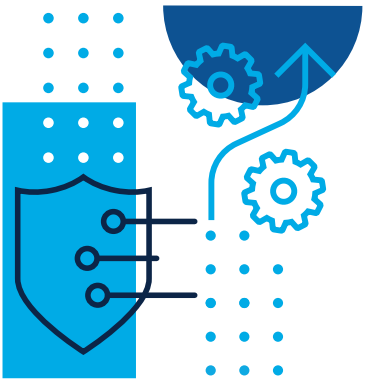
Adoption improves operational efficiency, enabling faster threat detection and response with minimal retraining for security teams. Graylog's user-friendly interface promotes cross-functional collaboration, while flexible deployment minimizes disruption during implementation.

Risk

Organizations with heavily customized legacy systems may face integration challenges, especially during migration. Proper planning and securing support are essential to ensure a smooth transition and avoid potential security gaps.

01 Solution Value

THE SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) market is transforming, driven by evolving cyber threats, increasing IT complexity, and vendor consolidations reshaping the landscape. As attacks against organizations become more frequent and sophisticated, the need for agile and responsive security solutions is growing. Many legacy SIEM systems need help to meet modern security demands, particularly for mid-to-large enterprises (up to $5B in annual revenue). This shift allows organizations to reassess their security strategies and adopt next-generation solutions that deliver greater efficiency and simplicity without the burdens of traditional SIEM deployments.



Re-evaluating and upgrading a SIEM solution offers clear business value. Organizations can enhance their threat detection and response capabilities, maintain regulatory compliance, and optimize operational efficiency. However, many existing solutions come with additional features that, while valuable to some organizations, may add complexity, leading to implementation challenges, underutilization, and diminishing returns on investment.

Re-evaluating and upgrading a SIEM solution offers clear business value. Organizations can enhance their threat detection and response capabilities, maintain regulatory compliance, and optimize operational efficiency.

02 Urgency & Risk

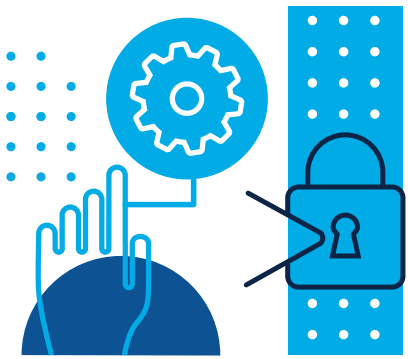
THE RAPID EVOLUTION OF CYBER THREATS and ongoing vendor consolidations in the SIEM market make it critical for organizations to reassess their security strategies. The urgency to deploy an effective SIEM solution is driven by the need to mitigate risks that can result in financial, operational, and reputational damage.

Urgency

For mid-to-large enterprises, especially in highly regulated industries like finance and healthcare, choosing a stable and reliable SIEM vendor is essential. Delaying action increases the risk of undetected breaches, which can escalate into serious security incidents, regulatory fines, and loss of customer trust. Organizations that act swiftly are better positioned to handle emerging threats and maintain a competitive edge.

Risk

Switching SIEM solutions presents risks that require careful management. Market consolidations can force unplanned vendor changes, and poorly managed transitions can lead to operational disruptions, increased costs, and potential security gaps. Organizations should prioritize robust support during migration, seeking vendors like Graylog that offer comprehensive onboarding services, parallel operations during transition, and clear planning to ensure successful deployment.

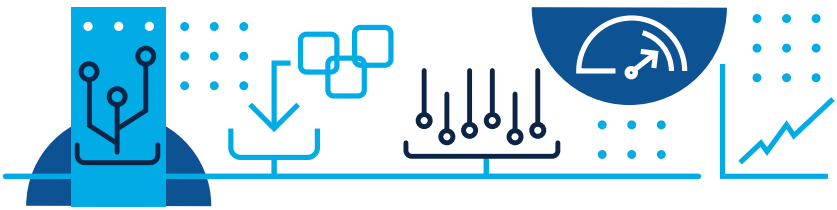


Delaying action increases the risk of undetected breaches, which can escalate into serious security incidents, regulatory fines, and loss of customer trust.

03 Benefits

IMPLEMENTING GRAYLOG'S SIEM SOLUTION PROVIDES mid-to-large enterprises with immediate operational improvements and long-term strategic advantages, tailored to meet the evolving needs of modern security teams. Key benefits include:

- **Deployment Flexibility:** Graylog allows organizations to choose the most suitable deployment model—on-premises, private, or public cloud—without compromising essential features, aligning the SIEM solution with specific operational and security needs.
- **Enhanced analyst experience:** Intuitive dashboards and streamlined workflows reduce the learning curve for analysts, increasing threat detection and response efficiency by allowing them to focus on security rather than navigating complex tools.
- **Lower total cost of ownership (TCO):** Graylog's unified platform minimizes licensing costs and long-term expenses through its straightforward deployment, ensuring a cost-effective security solution over the full three-year TCO.
- **Simplicity over complexity:** By focusing on essential features and avoiding unnecessary add-ons, Graylog provides robust security without introducing operational inefficiencies or coverage gaps.
- **API security monitoring:** Integrates with API security tools to provide visibility into potential threats, enabling faster detection and response to suspicious behavior.
- **Global deployment and support:** Graylog's strong global presence ensures compliance with regional regulations and provides support across international markets, crucial for organizations operating in multiple jurisdictions.
- **Continuous platform advancement:** Regular updates with new features like advanced anomaly detection, deeper API integration, and user-friendly automation tools keep Graylog effective amid evolving security challenges.

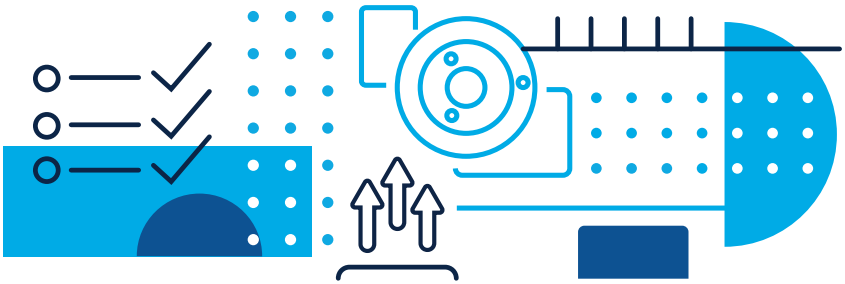


04 Best Practices

A SUCCESSFUL SIEM DEPLOYMENT requires strategic planning and operational execution. Following these best practices helps reduce disruption, leverage existing infrastructure, and maximize the platform's capabilities:

- **Conduct a needs assessment:** Define your security needs and objectives to ensure the SIEM aligns with your requirements and business goals.
- **Plan for parallel operations:** Minimize risks by running the new SIEM alongside the existing one during migration, allowing for a seamless transition.
- **Invest in training and support:** Train security analysts on the new platform and utilize onboarding services to accelerate adoption and optimize performance.
- **Integrate and automate:** Connect the new SIEM with existing security tools, such as IDS and EDR platforms. Automate tasks like log correlation and alerting to enhance efficiency.
- **Regularly review and optimize:** Continuously monitor system performance and adjust as needed to ensure the SIEM evolves with your security requirements.

By adhering to these practices, organizations can fully leverage the SIEM's capabilities, achieving a robust and effective security posture while minimizing the risks associated with SIEM deployment.



05 Organizational Impact

DEPLOYING THE GRAYLOG SIEM SOLUTION can enhance an organization's security posture, operational efficiency, compliance, and business resilience. Switching SIEMs requires careful planning to ensure smooth integration with existing processes and minimal impact on internal teams.

To maximize the solution's effectiveness and manage data integration and costs, consider the following best practices:

Optimize data integration: Identify and prioritize critical data sources for integration into Graylog, balancing coverage with cost-effective management.

Balance metrics and costs: Evaluate trade-offs between detailed security metrics and associated data storage/licensing costs. Use Graylog's flexible data management to optimize both insights and budget.

Targeted training: Provide specialized training for security teams, focusing on data handling capabilities and fine-tuning the system to meet performance and cost goals.

Continuous monitoring: Regularly review data practices to adapt to evolving security needs and budget constraints, ensuring ongoing balance between effectiveness and cost.

Graylog's global presence offers tailored support throughout deployment, helping security teams fully leverage the platform without overspending on data storage. This support aids in continuous monitoring and adaptation, positioning Graylog as a partner for organizations aiming to enhance security efficiently.

People Impact

Graylog's SIEM integrates seamlessly with existing security, IT, and technical teams, minimizing operational disruption. While some training is needed, its intuitive interface shortens the learning curve, with free on-demand training available.

06 Investment Outlook

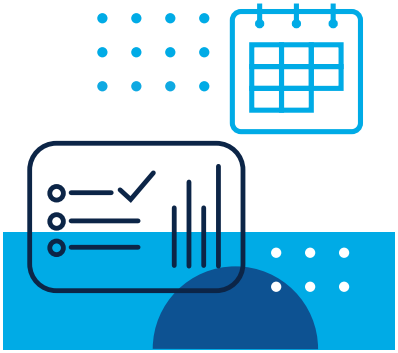
GRAYLOG'S SCALABLE AND ADAPTABLE SOLUTION is designed for mid-to-large enterprises, handling growing data volumes and emerging threats while maintaining predictable costs. The volume-based licensing model allows organizations to choose tiers that match their current processing needs and scale as necessary.

When considering the rough order of magnitude (ROM) spending, initial costs typically include licensing fees, onboarding, and self-paced training. Organizations with more complex requirements may need to budget for additional services. However, these upfront investments are manageable, especially when weighed against the potential long-term cost savings and operational efficiencies Graylog provides. With rapid integration and automation, value can be realized within the first few months, expediting ROI. Executives can confidently incorporate Graylog into their budget using a ROM estimate, knowing that ongoing costs will remain aligned with the platform's value.

When considering the rough order of magnitude (ROM) spending, initial costs typically include licensing fees, onboarding, and self-paced training. Organizations with more complex requirements may need to budget for additional services.

07 Solution Timeline

GRAYLOG'S SIEM SOLUTION CAN BE IMPLEMENTED within a relatively short timeframe, typically a few weeks to a couple of months, depending on the complexity of the existing infrastructure. Key factors affecting the timeline include integration with other security tools and the use of parallel operations during the transition. Graylog's global support and comprehensive onboarding services streamline the process, minimizing disruption to daily operations.



Future Considerations

In the next three years, organizations can expect continuous innovation from Graylog, including enhanced automation, expanded API security, and deeper integration capabilities. These developments align with the evolving cybersecurity landscape, ensuring that Graylog remains a reliable, forward-thinking partner for mid-to-large enterprises

In the next three years, organizations can expect continuous innovation from Graylog, including enhanced automation, expanded API security, and deeper integration capabilities.

08 Analyst's Take

THE SIEM SECTOR IS CRUCIAL in today's cybersecurity landscape, providing essential threat detection and response tools. As the market evolves, solutions that combine robust functionality with operational simplicity are increasingly valuable. Graylog's offering is particularly well-suited for mid-to-large enterprises seeking flexibility without compromising performance. Its comprehensive features make Graylog a strong choice for enhancing security posture.

Graylog's market leadership is highlighted by its recognition as a Leader and Fast Mover in the Innovation/Feature Play quadrant of the GigaOm Radar. This positioning reflects Graylog's commitment to continuous innovation and its effectiveness in addressing today's security challenges. For organizations focused on staying ahead of emerging threats, Graylog represents a top-tier option that delivers both advanced capabilities and operational efficiency.

Report Methodology | graylog

THIS GIGAOM CXO DECISION BRIEF ANALYZES a specific technology and related solution to provide executive decision-makers with the necessary information to drive successful IT strategies that align with the business. The report focuses on large impact zones often overlooked in technical research, yielding enhanced insight and mitigating risk. We work closely with vendors to identify the value and benefits of specific solutions and to lay out best practices that enable organizations to drive a successful decision process.

About Howard Holton

HOWARD HOLTON IS AN ANALYST AT GIGAOM. He has worked in IT for three decades, the last half in executive leadership, as a CIO and CTO. He has been an engineer, an architect, and a leader in telecom, health care, automotive, retail, legal, and technology.

In the last decade, Howard focused on cloud technology and economics, data analytics, and digital transformation. As CTO of Hitachi Vantara, he spent his time developing digital transformation, IT, and data strategies for Fortune 1000 companies and global governments.

His years at Rheem Manufacturing, Hitachi Vantara, and others provided the experience that helped him develop a mind for leadership—the successful execution of vision and culture to inspire. Successful leadership is all about maximizing your team's potential, as Howard has demonstrated over the course of his career.

Howard is also a technologist at heart; passionate about how data science and new technologies can be used to accelerate time-to-market and better serve the customer, now and in the future. Howard has been a trusted advisor and agent of change to a number of organizations, bringing vision and successful execution to internal and external customers alike.

GIGAOM

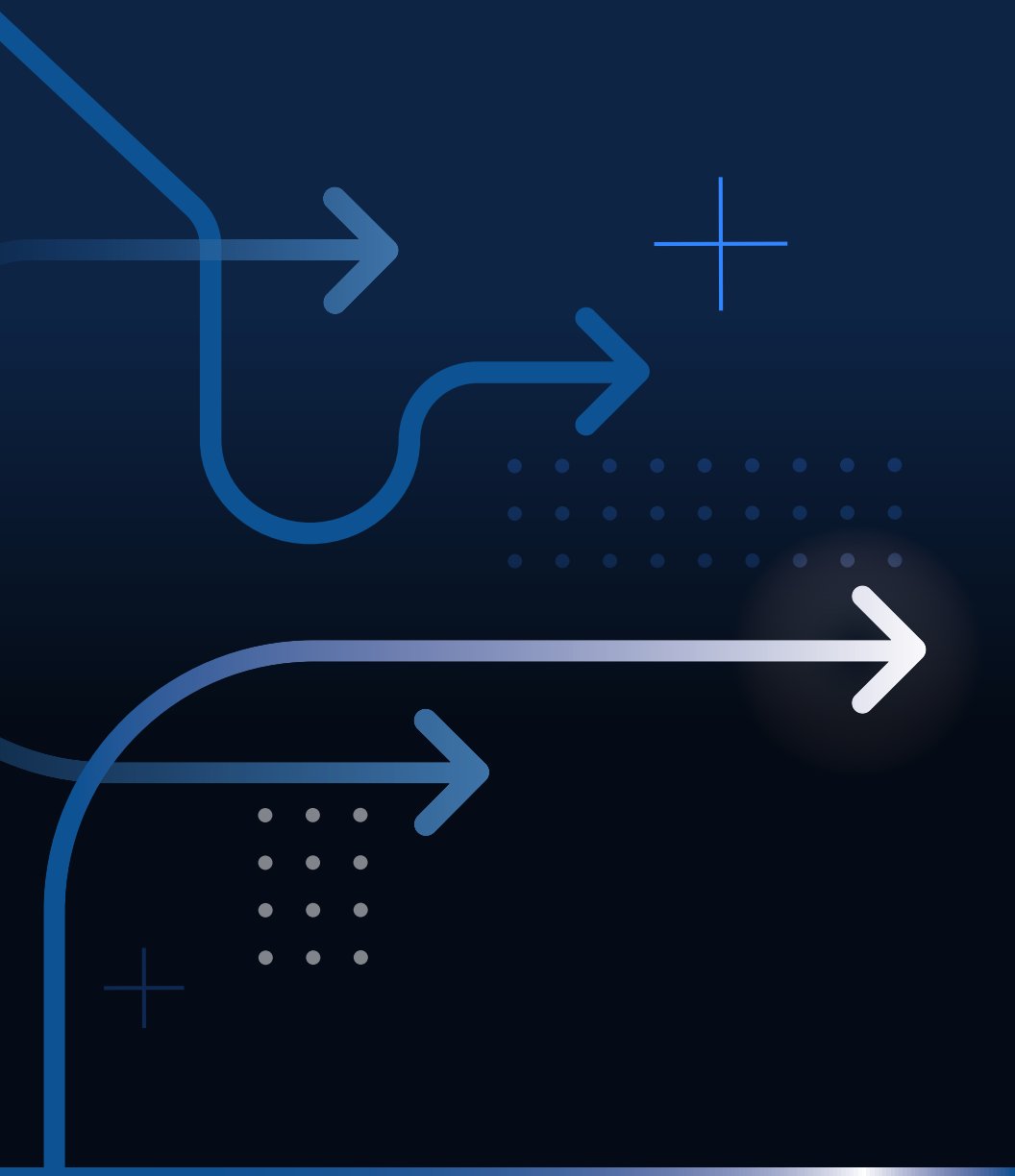
About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.


GIGA
OM



GIGAOM

GigaOm democratizes access to strategic, engineering-led technology research. We enable businesses to innovate at the speed of the market by helping them to grasp new technologies, upskill teams, and anticipate opportunities and challenges. The GigaOm platform changes the game, by unlocking deep technical insight and making it accessible to all.