Enterprise Strategy Group™
by TechTarget

ECONOMIC VALIDATION

# Analyzing the Economic Benefits of Graylog Security

## Reducing Operational Complexity, Speeding Time to Value, and Reducing Risk Versus Alternative On-premises SIEM Solutions, Resulting in a Return on Investment of 158% to 263%

By Aviv Kaufmann, Practice Director and Principal Validation Analyst
Enterprise Strategy Group

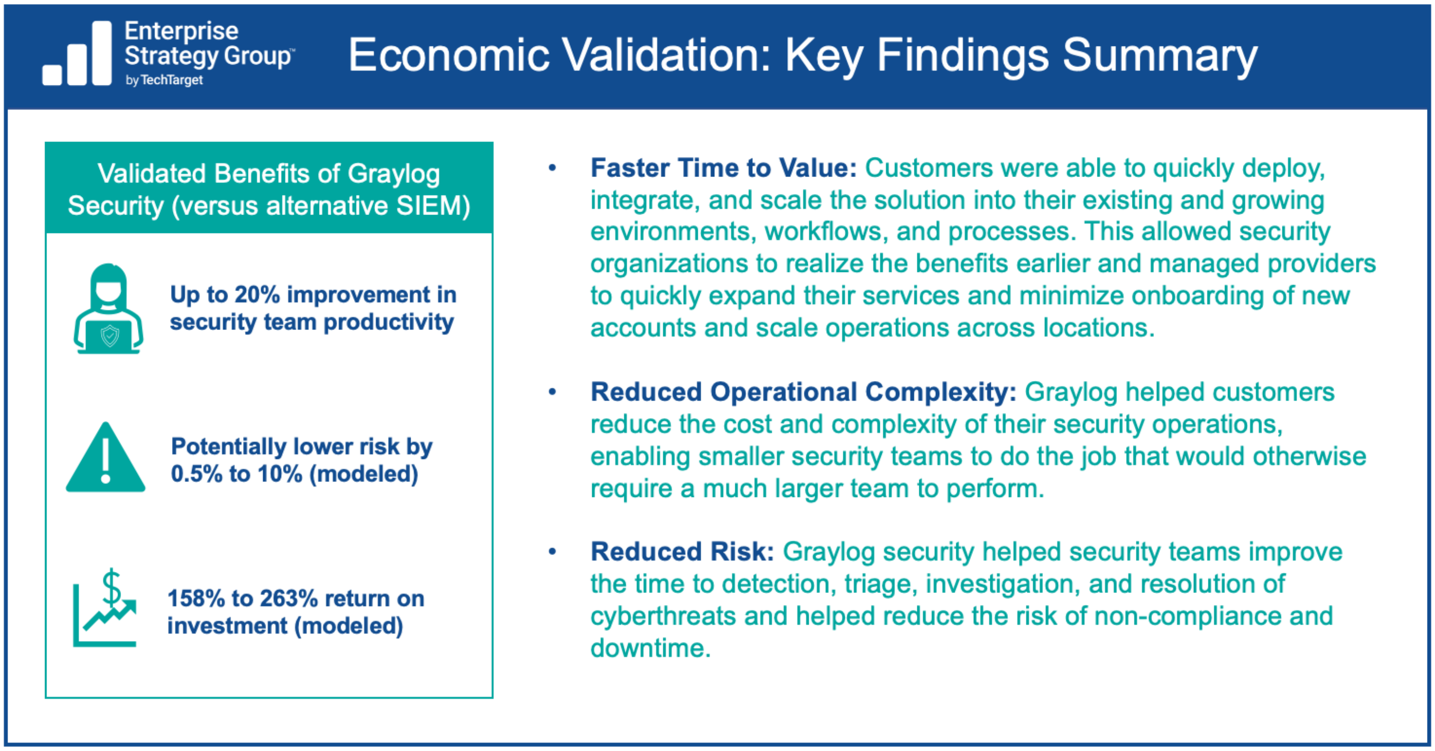
September 2023

This Enterprise Strategy Group Economic Validation was commissioned by Graylog and is distributed under license from TechTarget, Inc.

# Contents

# Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group focused on the quantitative and qualitative benefits organizations can expect by using Graylog Security rather than alternative on-premises security information and event management (SIEM) solutions to reduce operational complexity, speed operations, and better protect their organization.



Enterprise Strategy Group by TechTarget

**Economic Validation: Key Findings Summary**

**Validated Benefits of Graylog Security (versus alternative SIEM)**

**Up to 20% improvement in security team productivity**

**Potentially lower risk by 0.5% to 10% (modeled)**

**158% to 263% return on investment (modeled)**

- **Faster Time to Value:** Customers were able to quickly deploy, integrate, and scale the solution into their existing and growing environments, workflows, and processes. This allowed security organizations to realize the benefits earlier and managed providers to quickly expand their services and minimize onboarding of new accounts and scale operations across locations.
- **Reduced Operational Complexity:** Graylog helped customers reduce the cost and complexity of their security operations, enabling smaller security teams to do the job that would otherwise require a much larger team to perform.
- **Reduced Risk:** Graylog security helped security teams improve the time to detection, triage, investigation, and resolution of cyberthreats and helped reduce the risk of non-compliance and downtime.

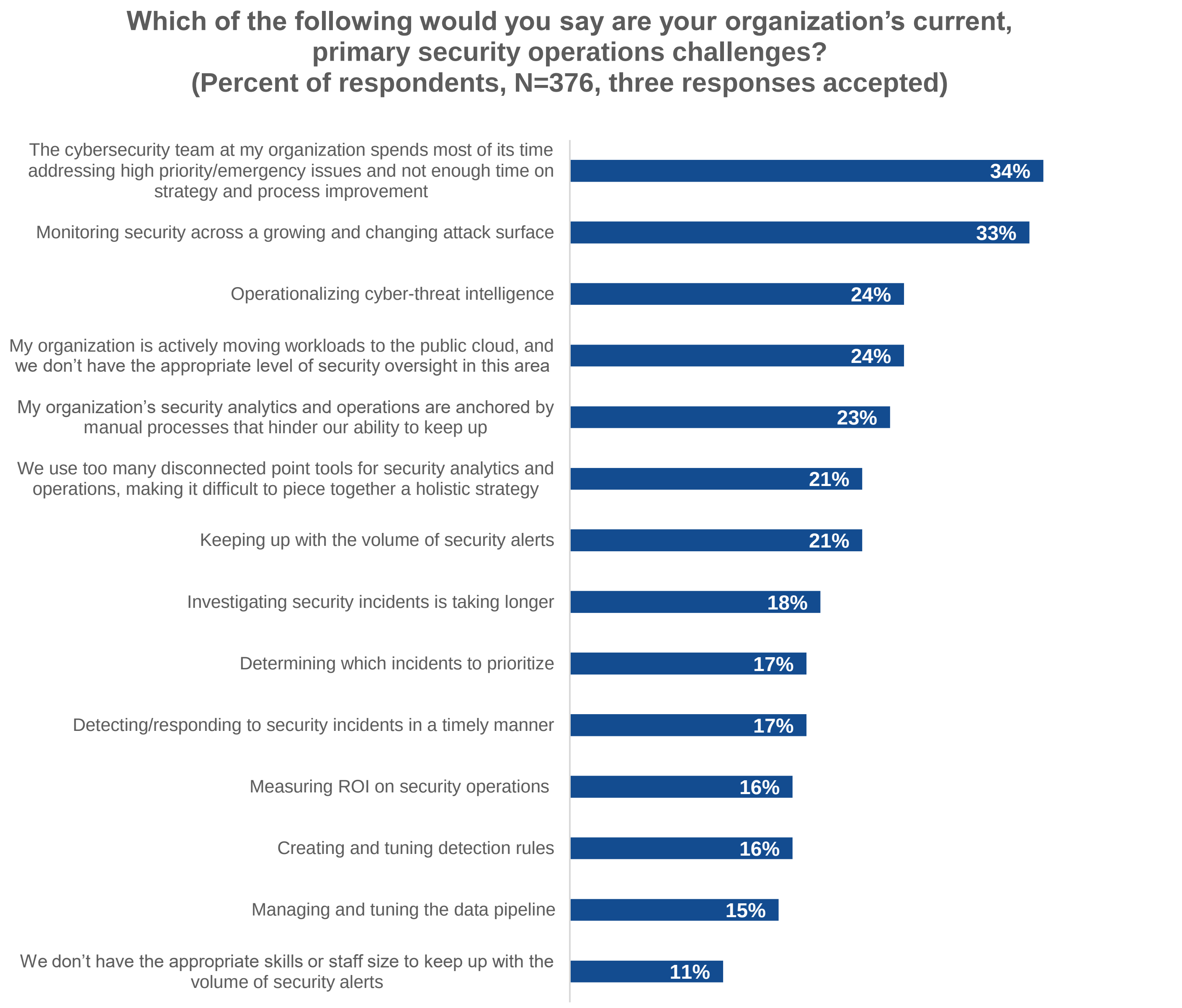
## Challenges

Today's fast paced, digitally transformed businesses rely on the expanded use of networks, devices, and applications to seamlessly deliver services and enable agile operations across the data center, edge, and cloud. This has resulted in an expanded attack surface and an exponential increase in the volume and velocity of generated log data that is generated. This, combined with the increasing variety and complexity of potential cyber threats, has led to a cybersecurity challenge for security organizations and managed security providers.

Security teams and providers need to move fast to identify, investigate, and remediate threats but have limited security resources, often have invested in too many tools, have established complex workflows, and need more visibility into the attack surface. Enterprise Strategy Group research identifies that some of the top security operations challenges include organizations reactively addressing security issues, struggling to operationalize cyber threat intelligence, not having the ability to provide security services for the public cloud, being slowed by manual processes, and leveraging too many security tools to get a holistic view of threats. Diving deeper into this list reveals that these teams need help to keep up with the volume of security alerts, investigate in a timely manner, and prioritize threats.[1]

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

**Figure 1.** Top Security Operations Challenges



*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

Many organizations have turned to feeding their security and log information into SIEM solutions to help successfully address some of their security operations challenges. But as the number of information sources multiplies and the amount of data generated by these sources rapidly grows, traditional SIEM solutions designed to be run on premises can become complex and costly to operate. It is difficult to predict the expected costs, often based on the volume of data ingesed or the number of devices monitored. Traditional SIEMs built for on-premises operations and tied to infrastructure offer limited functionality in the cloud and are challenging to scale. There are open source SIEMs available that help to limit costs when getting started. Still, as organizational needs scale, these open source SIEMs often limit functionality, visibility, and agility due to the increased complexity of solutions that do not include support. Suppose a SIEM is not designed to scale in the cloud and does not have enough customizability and intelligence built in. In that case, built-in teams can often suffer from alert fatigue. They will eventually be forced to increase complexity and cost through additional point tools and security team attention.

## The Solution: Graylog Security

Graylog Security combines SIEM, threat intelligence, and anomaly detection capabilities into a single on-premises or public cloud-deployed cybersecurity solution that can help organizations bolster their security posture. Built using the principles for designing Graylog Enterprise, its flagship centralized logging solution, Graylog Security allows security analysts to aggregate logs from any number of sources, search through logs easily, save and audit searches through logs, and write queries with an easy-to-use language.

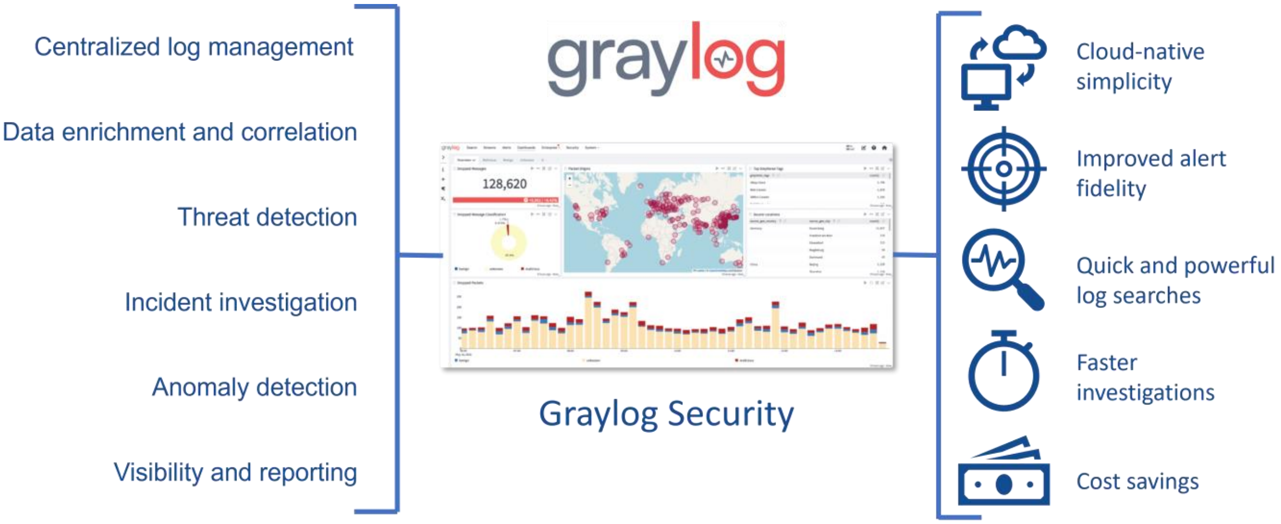
This is accomplished via Graylog's data transformation pipeline, which normalizes all data ingested into a common format, regardless of the source. Organizations can also ingest data from other sources, such as intelligence feeds, to more quickly research potential threats and anomalies.

To facilitate identification and analysis, Graylog enables organizations to conduct correlations to identify potential threats more quickly than if an organization conducted a manual drive analysis via trial and error. With the solution's machine learning (ML) anomaly detection engine, organizations can continuously run user and entity behavior analytics and uncover anomalies.

With Graylog Security's capabilities, organizations can strengthen their security by minimizing the time to detect threats and anomalies that deserve attention while filtering out the noise. Shorter times to detect translate into decreased mean time to resolution (MTTR). Resolving detected threats and anomalies more quickly minimizes gaps in an organization's security posture. Graylog Security's capabilities, accessible via a single interface, enable organizations to simplify their overall SIEM infrastructure and security operations workflows, resulting in lower overhead and costs.

In addition, gaps in cybersecurity skills can shrink as Graylog Security provides the tools and interfaces to ensure that any security analyst can immediately contribute and help strengthen the organization's security posture.

**Figure 2.** Graylog Security



*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

# Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative analysis of the Graylog Security solution. ESG's process is a proven method for understanding, validating, quantifying, and modeling the value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation.

ESG conducted in-depth interviews with end users to better understand and quantify how the use of Graylog Security has impacted their organizations, particularly in comparison with previously deployed and/or experienced SIEM solutions. ESG also reviewed demonstrations, vendor-created technical documentation, and existing case studies and leveraged our expert analyst opinions and knowledge of the industry, markets, and alternative technologies. The qualitative and quantitative findings were then used as the basis for a simple economic analysis that predicts the potential savings and return on investment (ROI) for a modeled organization.

## Graylog Security Economic Overview

Enterprise Strategy Group's economic analysis revealed that Graylog Security provided its customers with significant savings and benefits in the following categories:

- **Faster Time to Value** – Graylog Security was faster to deploy, configure, customize, learn, and use than alternative SIEM solutions.
- **Lower Cost of Security Operations** – Security teams found that Graylog Security reduced complexity and sped operations, enabling them to achieve more with smaller groups.
- **Reduced Risk to the Organization** – Graylog Security helped reduce risk to the organization by providing faster resolution of security and support issues and reducing the risk of non-compliance.

### Faster Time to Value

Graylog Security gave customers exceptional time to value, meaning they could quickly deploy, integrate, and scale the solution into their existing and growing environments, workflows, and processes. This enabled security organizations to realize the benefits earlier and managed providers to quickly expand their services and minimize the onboarding of new accounts while scaling operations across locations.

- **Faster deployments** – Graylog provided customers with immediate out-of-the-box value. Hardware-based solutions came preconfigured, eliminating hours of effort to install, configure, and test. Since Graylog Security was built with cloud-native capabilities, SaaS solutions could be deployed in minutes and easily scaled up and back as needed. Customers reported excellent support from professional services teams, resulting in faster deployment and quick and effective initial solution customization. When compared to their experience with alternative SIEMs, customers felt Graylog required less training, and the included content made it possible to start getting valuable insight from logs faster than legacy SIEMs. They could leverage pre-built Graylog Illuminate content packs and custom dashboards to quickly extract value from OS, firewall, and security tools' logs without building these capabilities independently.

> **"Graylog was much simpler to deploy than many of the alternatives. Everything from not having to deploy infrastructure to simpler configuration and automation made it faster for us."**

- **Faster time to value** – Managed security providers, security monitoring services, and support teams could integrate Graylog into their operations quickly and easily, quickly building scalable services into their offerings. The automation and flexibility provided by Graylog enabled them to incorporate Graylog swiftly into their workflows and deliver value to their customers. Graylog integrated with their other tools and enabled these teams to provide improved detection, investigation, and support for their customers much faster than if they were to try to build these capabilities themselves on other SIEM platforms. Security teams benefited from earlier protection at newly deployed sites. Managed security providers could take advantage of new business opportunities much quicker and impress customers with their quick initial deployment times.

> **"Graylog is built API-first, so we can build absolutely anything we want on top of it without restrictions. This flexibility is super helpful, and it's a night and day difference to the alternatives."**

- **Faster time to hybrid cloud operations** – Because Graylog Security offers the same feature set and lockstep development between on-prem (self-managed) and cloud versions, organizations could leverage both deployment options without worrying about the differences in operations or support. Customers shared that some alternative SIEM providers had depreciated assets between versions, offered limited functionality or scalability for their cloud versions, and required added complexity and additional learning when using the different versions, which they felt limited their flexibility. They also mentioned that Graylog Security was straightforward to scale both on premises and in the cloud using the API and a few lines of code. In contrast, other solutions required many more steps, some limiting their ability to scale.
- **Faster investigations and searches** – One of the most significant benefits reported by customers compared to alternative SIEMs was Graylog's ability to perform parsing and searches across much larger data sets in less time and with less effort. Fast searches and search filters made it possible to refine terabytes of data in near-real time. Equivalent searches on alternative SIEMs required customers to "sit and wait" while the query was executed, with them sometimes leaving and coming back later. Customers could also enrich their data sets with the results from other sources such as WHOIS, IP Geolocation, threat intel, and different data sets. One organization selected Graylog because it offered **"easy centralization, easy parsing, and fast/scalable search and the ease at which [they] could drill down into the data."** This unique ability to search larger data sets faster helped to detect and resolve cybersecurity, network, infrastructure, and application issues quicker, increasing the operational effectiveness of resources, improving application and service product quality, and reducing risk to the organizations.

> **"Graylog makes it very easy to get the data you want in the format you want it in. This gives our team more velocity and success in what we do daily."**

## Lower Cost of Security Operations

Customers primarily chose Graylog because it helped them reduce the cost and complexity of their security operations. This enabled smaller security teams to perform the job that would otherwise require a much larger team. Graylog Security helped make teams more operationally efficient through the following benefits:

- **Fewer tools to manage** – Graylog Security combines the capabilities of SIEM, threat intelligence, and anomaly detection capabilities into a single tool. In addition to threat intelligence and anomaly detection, one customer suffering from tool sprawl could use Graylog to eliminate the need for many tools such as IT service management, log management, search and analytics engine, data processing platform, and visualization tools for reporting. This helped them to minimize licensing costs, reduce complexity, and maximize the effectiveness of their IT and security teams.

> **"The other SIEMs that we have used were overpriced and overcomplicated. Graylog has improved both [cost and complexity] for us."**

- **Reduced complexity** – When asked to compare Graylog Security to their previous experiences with SIEM solutions, customers reported that Graylog required management of fewer components and reduced complexity for their security teams. The easy integration of log sources and intuitive UI made learning and using Graylog faster so that even less experienced resources could quickly come up to speed. Some customers could rely on simple queries without learning SQL or proprietary language. Graylog's built-in visualizations, search templates, investigation workflows, and alert and correlation customization wizard helped save time and effort, and built-in archiving of older data reduced the complexity of dealing with data lifecycle management.

> **"Graylog is far less complex [than alternatives] from the start of integrating a log source to the finished process of the log source and everything in between."**

- **Less time parsing and searching data** – As described earlier, IT and security teams could use Graylog to reduce the time spent parsing and searching data, especially at scale and looking further back into historical context before events. Teams also reported that they could use parameterized searches to drill down deeper into the data and provide better context and insight into the operations they needed to perform. In addition, teams felt that Graylog provided them with more of a real-time view of the data they were searching compared to other SIEM solutions. One customer shared, **"We have had issues with other platforms where log sources and alerts would be delayed, but with Graylog, the logs are in real time and constant without interruption."**
- **Automated actions and API** – Customers reported that the automation provided by Graylog and the ability to build customizations for almost any function through the API made it possible to search more data in less time, reduce extra steps, and automate repeatable tasks required to collect, normalize, and visualize logs. Teams could save and share parameterized searches to ensure consistency in their investigations, automate cyber threat resolutions and Dev/Ops operations, and nearly fully automate deployment and scaling for new instances of Graylog services.

> **"The automation allows our team to remain small and nimble while being just as effective as a larger team."**

- **Reduced alert fatigue** – Teams were able to customize alert criteria to ensure that only critical alerts required immediate attention, helping to free up resources to focus on more time-sensitive tasks. These teams could receive vital alerts via email, Slack, text, and other methods. While one customer shared with us that Graylog provided only a fraction of the built-in connectors and out-of-the-box alerts that came with some of the more expensive SIEMs, they felt they could better customize alerts by building them on their own with Graylog. Since they had better knowledge of their environment and team, they could build more effective intelligence into the logic and felt that this helped to eliminate a lot of the alert noise that could be generated by relying on out-of-the-box alerts.
- **Integration with existing tools and workflows** – Another top reason customers chose Graylog over alternative solutions was that it gave them the flexibility to better adapt to custom and unique security requirements. Customers integrated with existing security orchestration, automation, and response (SOAR) and central threat intelligence (CTI) platforms to initiate workflows from critical correlation alerts and leveraged existing threat intelligence feeds to add deeper context to event log data. Prebuilt and custom dashboards and reports helped to inform various departments with insight derived from log sources that went far beyond cybersecurity to IT services, application developers, line-of-business decision-makers, and compliance departments.

> **"If you can search on it, you can create a widget. That widget goes into a dashboard and can then be run as a report—very straightforward."**

## Reduced Risk to the Organization

A critical aspect of any security product is how well it will help reduce cybersecurity risk for the organization. While Graylog security does a great job of protecting organizations from cybersecurity threats, we found that organizations were using it to minimize the risk to the business in other areas.

> **"We have used three different SIEM platforms in our services, and Graylog is the best so far. We are excited to move everyone to Graylog in the future."**

- **Improved time to resolution** – Graylog security helped security teams improve the time to detect, triage, investigate, and resolve cyber threats. Teams benefitted from faster detection by bringing in more sources, improving the context provided by threat intelligence feeds and enabling teams to remediate threats faster by integrating with SOAR for an automated response. Graylog's Investigation Workflows helped combine multiple searches into singular actions. Incident Investigation provided teams with a shared workspace to coordinate investigation efforts by consolidating data sets, reports, evidence, and contextualization so that less time was lost trying to share information through other means. Teams used Graylog Security to resolve support issues, compliance issues, application bugs, and performance issues, in addition to malware, security incidents, and insider threats.
- **ML Intelligence** – Graylog's anomaly detection ML engine continuously analyzes the environment and security behaviors and improves an organization's security posture over time. Customers could use correlation alerts to alert on complex issues requiring contextualized information and logical analysis across multiple logs and events. Graylog's ML intelligence helped to detect threats that otherwise may have gone unnoticed, helping security teams be more effective at identifying and protecting against threats.
- **Reduced risk of non-compliance** – Customers could use the integrated dashboards and automated reporting to help simplify compliance activities. The log archiving capabilities provided by Graylog helped organizations such as healthcare providers and financial institutions to cost-effectively retain more information to meet requirements better and avoid non-compliance audits and potential fines. These organizations could set longer retention times to better comply with the requirements of internal audits and quickly reimport the log data if and when needed to prove compliance. In addition, customers could enforce and demonstrate compliance by tracking user activity on log data, including audit logs, authentication tracking, access management, and user behavior analysis.

> **"We have a dashboard created for compliance audit requests that come from our customers every year, so we just run the audit report and send it off to them whenever they need it."**

- **Improved troubleshooting and reduced downtime** – While Graylog Security's primary purpose is protecting against cyber threats, Graylog was also used by application development and support teams to troubleshoot full application stacks and pinpoint issues that may result in bugs, vulnerabilities, and potential downtime. Development teams were able to provide custom dashboards to assist customer support and engineering teams with information relating to new code releases. If IT downtime events occurred, Graylog searches could be used against the historical network, infrastructure, and application logs to correlate issues and find root causes to speed time to recovery.

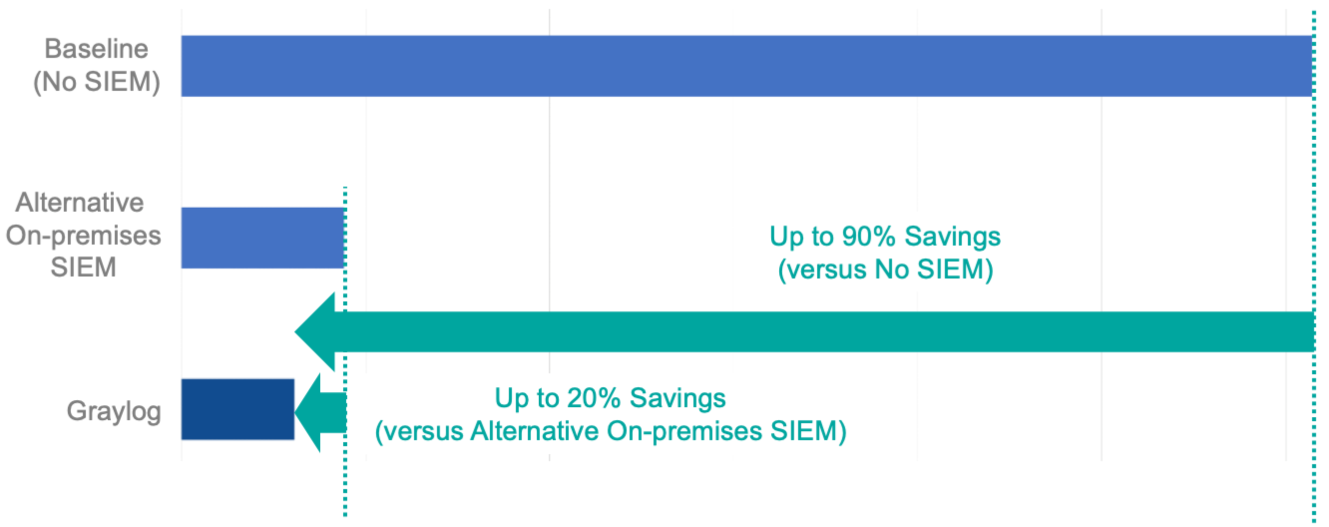
## Enterprise Strategy Group Analysis

Enterprise Strategy Group (ESG) leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a three-year TCO/ROI model that compares the costs and benefits of providing security services with Graylog Security versus using a traditional on-premises SIEM solution. ESG's interviews with customers who have recently made the transition, combined with experience and expertise in economic modeling and technical validation of security technologies, helped to form the basis for our modeled scenario.

Our assumption was based on a composite organization operating with an 8-person security team and ingesting an average of 100GB of log data daily. By sizing out the annual cost of the solutions based on known customer spending, we assumed that Graylog Security provided a 21% lower cost (savings varied among SIEM solutions between an equivalent price and 2x the cost).

To model operational savings, we assumed that the security team spent about 20% of their time on active SIEM-related activities, including responding to alerts and investigating threats and other issues by searching through log events. Data obtained via interview confirmed that without Graylog Security, customers felt they would require a security team that was at least 10x as large. If they were to use their previous SIEM only, they would still need to grow their team size by 2 people. Modelling out the operational savings, Graylog provided up to a 90% savings over the baseline (no SIEM) and a 20% savings over using an alternative on-premises SIEM solution.

**Figure 3.** Expected Operational Savings



*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

While we were unable to collect quantified risk reduction through customer-shared metrics, we leveraged our proprietary models to predict a very conservative reduction in risk provided by Graylog over alternative SIEMs that could be achieved through a combination of being able to pull in more sources, retain more data, provide near-real-time access to log data, provide improved context, and accelerate searches and ongoing investigations. Our conservative results and assumptions are summarized in Table 1.

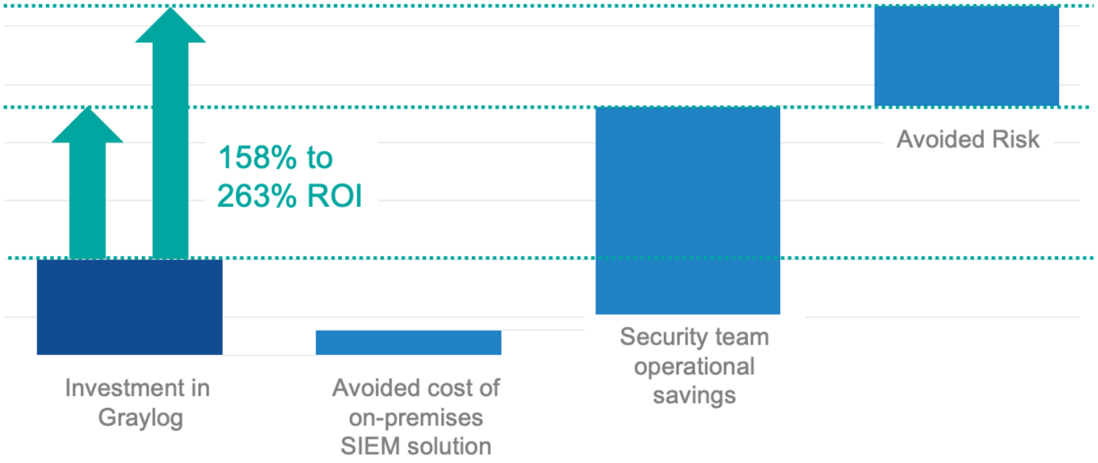
**Table 1.** ESG Modeled Expected Annual Risk

| | Baseline (No SIEM) | Alternative SIEM Solution | Graylog | Graylog Reduction in Risk (vs. alternative SIEM) | Graylog Advantage |
|---|---|---|---|---|---|
| **Risk of a cybersecurity event** | $1.287M | $64.4K | $57.9K | **$6.4K** | ESG assumed a 0.5% improvement over the 95% SIEM improvement assumption based on the ability for faster searches and custom alerts. |
| **Risk of compliance audits and fines** | $816.5K | $653.2K | $645.0K | **$8.2K** | ESG assumed a 1% improvement over the 20% SIEM improvement assumption based on the ability for faster searches and archiving advantages. |
| **Risk of IT downtime** | $200K | $100K | $80K | **$20K** | ESG assumed a 10% improvement over the 50% SIEM improvement assumption based on the ability for faster searches, custom alerts, and more straightforward integration of log files. |

*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

Putting this together, ESG calculated an expected annual ROI for Graylog Security compared to alternative on-premises SIEM solutions. The resulting ROI (shown in Figure 5) ranged from 158% (which conservatively excludes the benefits of avoided risk) to 263% (including the potential benefit of avoided risk).

**Figure 4.** Expected Return on Investment



*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

### Issues to Consider

While Enterprise Strategy Group's models are built in good faith upon conservative, credible, and validated assumptions, no single modeled scenario will ever represent every potential environment. The costs and benefits received from a Graylog Security deployment will depend on the details of your requirements and practice. Enterprise Strategy Group recommends that you analyze available products and consult with your Graylog representative to understand and discuss the differences between the solutions proven through your proof-of-concept testing.

## Conclusion

As organizations modernize their IT environments, security teams are asked to rethink their tools to support hybrid cloud operations. While the practices of securing infrastructure and applications on-premises and in the cloud benefit from a unified approach, the tools that organizations have relied on in the past may not be ready to deliver the same simplicity, functionality, visibility, scalability, and service levels once moved to the cloud. While this may concern some SIEMs, Enterprise Strategy Group validated that Graylog Security offers the same feature set and lockstep development between on-prem (self-managed) and cloud versions, making it an excellent choice for modern hybrid cloud operations.

Our validation with Graylog Security customers revealed that compared to previously deployed SIEM solutions, Graylog Security provided faster time to value and reduced cost, operational complexity, and risk. Our modeled scenario predicts that Graylog Security can be operated by teams up to 20% smaller than required with some alternative SIEMs and expected an annual ROI of 158% to 263%.

At a time when security organizations are being asked to do more with less, maximize the productivity of existing security resources, and minimize the number and complexity of tools, Enterprise Strategy Group recommends that you evaluate if Graylog Security is the right platform for you.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

**About Enterprise Strategy Group**
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com