International Journal of Advanced Engineering and Management Research

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Infrastructure Monitoring for the Resilience of Critical Infrastructure

Ferenc Bálint[1]
[1]University of Óbuda, Hungary,
Orcid ID: 0009-0009-8970-762X

doi.org/10.51505/ijaemr.2025.1519 URL: http://dx.doi.org/10.51505/ijaemr.2025.1519

Received: Nov 24, 2025 Accepted: Nov 29, 2025 Online Published: Dec 08, 2025

Abstract
Modern organizations rely on efficient monitoring solutions to safeguard the performance, security, and stability of their IT infrastructure in an increasingly connected world. The integration of advanced monitoring techniques has significantly shaped the evolution of IT security and operational efficiency, particularly in response to the growing complexities of modern infrastructures and cybersecurity threats. This article explores the historical development of infrastructure monitoring solutions, detailing the progression from traditional methods to the sophisticated, AI-powered tools used today.

Key IT monitoring tools, including Security Information and Event Management (SIEM), Security Information Monitoring (SIM), Application Performance Management (APM), and network and system monitoring solutions, form a robust framework for managing both security and performance. These tools have evolved to detect and mitigate threats, automate responses, and ensure the continuous performance and reliability of systems across industries.

The adoption of automation and the inclusion of Artificial Intelligence (AI) and Machine Learning (ML) into these monitoring platforms represent the most recent advancements in IT security. AI-driven solutions enable predictive threat detection, anomaly identification, and automated responses, improving operational efficiency while reducing false positives. These capabilities enhance not only the overall security posture but also the performance of critical infrastructure systems.

As the challenges of managing large-scale data, real-time analysis, and ever-evolving cyber threats grow, the integration of these monitoring tools is crucial for proactive risk management. By combining SIEM, SIM, APM, and AI-powered solutions, organizations can optimize their security and operational strategies, ensuring the resilience and protection of essential infrastructures in an increasingly complex cyber landscape.

Keywords: AI, application, attacks, challenges, cloud, critical infrastructure, cyberattack, cybersecurity, monitoring, performance, platform, risk, security, threats

Vol. 10, No. 06; 2025

ISSN: 2456-3676

1. Introduction

Critical infrastructures are fundamental to modern society, supporting essential services such as electricity, water and gas distribution, transportation, communication networks, and healthcare and financial systems. These systems are vulnerable to various risks, including cyberattacks, natural disasters, and technical failures, which can lead to severe economic and social consequences. Therefore, ensuring the security and continuous operation of these infrastructures is paramount in mitigating potential threats and maintaining stability.

Critical infrastructures face numerous security challenges, with primary threats originating from cybercriminals, terrorists, and even state actors aiming to disrupt or destroy essential systems. Natural disasters like storms, floods, and earthquakes also pose significant risks. Additionally, human errors and technical failures, if not properly managed, can lead to catastrophic consequences.

A wide array of security solutions is available to safeguard critical infrastructure. Cybersecurity measures such as firewalls, intrusion detection systems, and security protocols help defend against cyberattacks. For natural disasters, measures like emergency preparedness plans, strategic infrastructure placement, and reinforcing buildings and equipment are critical. To prevent human errors and technical failures, regular inspections, monitoring, and maintenance are necessary. In today's fast-paced, technology-driven world, continuous monitoring (24/7) is essential for identifying and addressing incidents before they escalate. Monitoring tools enable real-time surveillance, providing early alerts on security threats, system performance, and availability. These tools can also be used for optimizing system performance. AI-powered monitoring tools are becoming increasingly important, offering automation and insights to reduce false positives and enhance operational efficiency. As infrastructure grows more complex, the integration of AI and automation into monitoring systems becomes crucial for improving efficiency. AI allows for predictive threat detection, anomaly identification, and automated responses, reducing the reliance on human intervention and streamlining operations. Predictive insights from AI also help reduce false alarms and improve the accuracy of root cause analysis during incidents, enabling faster problem resolution.

Effective monitoring systems support a variety of IT processes such as incident management, problem management, change management, and data and capacity management. These systems span multiple layers, including network, operating system, application, storage, and database layers, ensuring comprehensive coverage. By automating the analysis of application logs, metrics, and events, monitoring tools can detect issues quickly and minimize manual involvement, allowing resources to be optimized.

As part of the monitoring system, Application Performance Management plays a vital role in ensuring the smooth operation of IT systems. APM solutions track the entire process of applications, from user interactions to backend systems, identifying bottlenecks or issues that might impact performance. For instance, APM can be used to monitor online store transactions,

Vol. 10, No. 06; 2025

ISSN: 2456-3676

detecting delays in response times or failures in database queries. This capability is crucial during high-demand periods like holidays or sales events, where automated scaling can ensure system performance remains stable. Successful monitoring requires a deep understanding of the system architecture, including components like databases, services, microservices, and third-party solutions. In today's multi-platform environment, mobile devices, web browsers, and security protections, such as biometric authentication or PIN codes, must also be considered. Monitoring tools must track these diverse environments to maintain a secure and functional system. As critical infrastructure systems become more integrated and complex, continuous monitoring is essential to ensure their security and performance. By leveraging modern monitoring tools, including AI and automation, organizations can effectively manage risks, optimize performance, and ensure the resilience of critical infrastructures. Effective monitoring is not just about tracking system health—it's about enabling proactive responses to incidents, minimizing downtime, and protecting essential services that support modern society.

2. Evolution of Infrastructure Monitoring Techniques

The history of infrastructure monitoring and automation shows how technology has evolved to meet the changing needs of different industries. In its early stages, organizations struggled to manage their expanding technological infrastructures, relying on basic, manual tools for network monitoring. This shifted dramatically with the introduction of automated solutions, marking a key turning point as businesses moved from reactive to proactive monitoring.

A major breakthrough came with the integration of artificial intelligence, which brought intelligent, adaptable monitoring systems capable of learning from data patterns, predicting issues, and responding dynamically to changing conditions. This technological leap increased the speed and accuracy of monitoring, transforming IT ecosystems into more dynamic and responsive environments.

Industries played a significant role in shaping this evolution. The rise of the digital era and the shift to virtualized environments and cloud platforms presented new challenges that demanded specialized monitoring solutions. In healthcare, for example, real-time monitoring became crucial for maintaining the performance and availability of critical applications. Meanwhile, in the financial sector, the need for monitoring tools that could secure large volumes of sensitive data led to advancements in security-focused monitoring.

By looking at these industry-specific dynamics, we gain valuable insights into the forces driving the development of infrastructure monitoring and automation. This historical context is essential for understanding how industries have influenced the modern landscape of IT infrastructure management.

Adoption trends provide further clarity on how organizations have embraced these technologies. As businesses transitioned to cloud-based infrastructures, they sought monitoring solutions that could handle dynamic cloud environments. The widespread adoption of cloud-native monitoring

Vol. 10, No. 06; 2025

ISSN: 2456-3676

tools became a key trend, as organizations prioritized ensuring the performance, availability, and security of applications in the cloud.
By examining how organizations navigated through these phases of adoption, we can better understand the broader trends in infrastructure monitoring and automation and the strategic decisions that have shaped IT management in the digital age.

3. Key Players in the Infrastructure Monitoring and Automation Landscape

The monitoring and automation landscape is heavily shaped by established leaders who have not only pioneered innovative solutions but also built a strong market presence. Companies like IBM, Microsoft, and Cisco have played a key role in defining the industry with their comprehensive monitoring and automation offerings. Microsoft, in particular, is notable for its System Centre suite, which includes System Centre Operations Manager (SCOM) and System Centre Orchestrator (SCORCH). These foundational tools help organizations achieve effective infrastructure monitoring and automation. SCOM, for example, offers end-to-end monitoring of applications and infrastructure, providing deep insights into performance and overall health. Understanding the influence of leaders like Microsoft is essential, as it helps organizations adopt proven solutions while expanding the scope of their enterprise application monitoring.

Alongside these established players, emerging innovators are disrupting the traditional monitoring and automation landscape with fresh perspectives and novel solutions to address evolving IT challenges. Companies such as Datadog, Splunk, and Dynatrace represent the innovative drive pushing the industry forward. Datadog, for example, has become a prominent name in cloud monitoring and analytics, offering unified visibility into the performance of applications, servers, and infrastructure. Recognizing the impact of emerging innovators is important for organizations seeking diverse solutions tailored to their specific IT needs.

Collaborations within the monitoring and automation sector create a dynamic ecosystem where joint efforts advance the development and integration of cutting-edge solutions. Partnerships between hardware providers, software developers, and cloud service providers foster a collaborative environment that enhances capabilities. For instance, partnerships between Cisco and major cloud service providers have resulted in integrated cloud-based monitoring solutions. Understanding the value of these strategic partnerships helps organizations choose the best monitoring and automation solutions that align with their overall IT strategies.

4. Introduction of Key Security Information Monitoring Tools

Effective monitoring is a cornerstone of any IT environment. When it comes to Security Information Monitoring, several advanced tools are available to help organizations protect critical infrastructures from cyber threats. These tools integrate with various IT systems, providing real-time monitoring, threat detection, and response capabilities. One of the leading platforms in this field is Microsoft Azure, specifically Azure Sentinel, but there are several other notable SIM tools on the market.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4.1 Azure Sentinel

Azure Sentinel is a cloud-native Security Information and Event Management solution developed by Microsoft that leverages artificial intelligence and machine learning to detect, investigate, and respond to security threats in real time. As a cloud-based platform, it provides scalability, flexibility, and seamless integration with both Microsoft solutions and third-party tools. Azure Sentinel's AI-powered threat detection capabilities enable it to identify anomalies and potential threats with greater precision. It continuously collects and analyzes data from various sources such as network traffic, applications, and endpoints, delivering real-time security analytics. Moreover, Sentinel automates responses to common threats using predefined playbooks, significantly reducing the manual workload for security teams. The integration with Microsoft 365 further enhances visibility across cloud, on-premises, and hybrid environments, ensuring a comprehensive security approach. Azure monitoring, in particular, plays a crucial role in fine-tuning alerts. System administrators can set threshold values to ensure that only genuine issues trigger notifications, helping to reduce alert noise and enabling quicker identification of real problems. Azure Monitor not only facilitates the analysis of data from cloud infrastructure but also supports intervention at the user level and through AI-powered assistance. When configuring alerts, it's essential to select the correct metrics and set appropriate thresholds. Regular monitoring and adjustment of these thresholds are vital to ensure that systems operate within the desired parameters, triggering alerts based on predefined rules that monitor specific metric values. Alert rules are a critical component of the system, as they initiate various actions when triggered. In some cases, AI can intervene, executing predefined steps to maintain uninterrupted system operation. Azure monitoring also tracks resources that have been specifically defined for observation. Alerts are activated when the conditions set in the alert setup are met and are resolved once those conditions are no longer present. The Action Group automates the process, sending notifications via SMS, email, or push notifications, and can initiate calls through services like Opsgenie. Additionally, alerts are retained for 30 days before being automatically deleted, ensuring efficient management of alert data.

4.2 Splunk

Splunk is one of the most well-known tools in the world of Security Information Monitoring. It excels at collecting, indexing, and analyzing machine data from various sources, providing security teams with actionable insights into potential vulnerabilities. Splunk ingests data from a wide array of sources, including applications, operating systems, network devices, and cloud environments. The platform's advanced analytics capabilities provide real-time threat intelligence, helping to detect complex cyber threats and attack patterns. Additionally, Splunk allows for customizable dashboards, enabling security professionals to tailor the platform's interface to their specific needs. It also integrates seamlessly with a wide variety of security tools and platforms, enhancing its monitoring and response capabilities. Splunk is highly scalable, making it suitable for both small businesses and large enterprises.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

4.3 IBM QRadar

IBM QRadar is a comprehensive SIEM tool that provides real-time security intelligence and automated incident detection. It is widely recognized for its powerful data collection, analysis, and correlation capabilities. QRadar integrates with threat intelligence feeds to enhance detection capabilities, giving security teams valuable insights into emerging threats. The platform normalizes data from various sources, making it easier to correlate and identify potential security incidents across different systems and devices. QRadar also automates the process of detecting, prioritizing, and managing security incidents, helping security teams respond faster and more efficiently. Furthermore, QRadar's pre-configured reports assist organizations in meeting regulatory compliance requirements, which is especially important in sectors like healthcare and finance.

4.4 LogRhythm

LogRhythm provides a unified platform for SIEM, log management, and network monitoring, with a focus on helping security teams detect and respond to threats more quickly. The platform continuously monitors data across an organization's network to detect potential security incidents in real-time. One of its standout features is User and Entity Behavior Analytics (UEBA), which helps detect insider threats by identifying anomalies in user or entity behavior. LogRhythm also offers automated responses to security incidents, reducing the time to address potential threats. Its ability to integrate with a wide range of data sources, including security logs, endpoint data, and network traffic, provides a unified view of an organization's security posture.

4.5 Rapid7 Insight IDR

Rapid7 Insight IDR is another SIEM tool that focuses on monitoring, detecting, and responding to security incidents. It simplifies security operations while providing actionable insights to security teams. The platform integrates Endpoint Detection and Response (EDR) capabilities to track and monitor endpoint activity, which is essential for identifying advanced persistent threats (APTs). InsightIDR uses behavioral analytics to detect malicious activities, such as abnormal login attempts or privilege escalation, and it provides continuous monitoring and automated incident response to quickly address vulnerabilities. The tool also integrates well with cloud services, making it suitable for hybrid and cloud-first environments.

4.6 Zabbix

Zabbix is an open-source monitoring solution used for monitoring the health and performance of IT infrastructures, including networks, servers, applications, and cloud services. Zabbix provides real-time monitoring, alerting, and reporting, allowing IT teams to detect potential problems early. It is scalable and customizable, offering extensive integration options, templates, and an intuitive web-based interface for managing monitoring tasks across large, distributed environments. Zabbix is suitable for medium to large enterprises seeking a free, scalable monitoring solution.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Figure 1: **Zabbix** is an open-source monitoring tool

https://uptrace.dev/tools/monitoring-tools-for-it (accessed Feb. 20, 2025)

4.7 McAfee Enterprise Security Manager (ESM)

McAfee Enterprise Security Manager is an enterprise-grade SIEM tool that provides real-time security monitoring and threat detection. It offers centralized event management, log collection, and security analytics, allowing security teams to detect and respond to incidents quickly. McAfee ESM is known for its high scalability, making it suitable for large organizations with complex security infrastructures.

In the battle against cyberattacks on critical infrastructures, the implementation of robust Security Information Monitoring tools is essential. These platforms provide real-time visibility, threat detection, and incident response, making them indispensable in defending against today's sophisticated cyber threats. For critical infrastructures, choosing the right SIM tool depends on the specific needs of the organization, the scale of operations, and the complexity of the infrastructure. However, the common goal remains the same: ensuring that security teams can quickly identify and mitigate risks before they lead to significant disruptions.

On the other hand, Application Performance Management is focused on monitoring and optimizing the performance of applications. APM tools allow organizations to proactively track the health of their applications, detect issues early, and improve performance for a smooth user experience. They continuously monitor key metrics such as response time, uptime, and

Vol. 10, No. 06; 2025

ISSN: 2456-3676

throughput. APM also offers root cause analysis, helping to pinpoint performance problems like slow database queries or inefficient code. Additionally, APM tools assess end-user experience, measuring how users interact with the application. When performance thresholds are exceeded, APM systems trigger alerts and diagnostics, providing real-time solutions. Furthermore, APM tools offer optimization recommendations to enhance efficiency and ensure smooth operation.

4.8 Dynatrace

Dynatrace is a leading application performance management solution that provides deep insights into the performance and health of applications, infrastructure, and user experience. It uses artificial intelligence to monitor the entire application lifecycle, from user experience to backend infrastructure. Dynatrace automatically detects performance bottlenecks, provides detailed root cause analysis, and offers real-time monitoring to ensure optimal application performance in complex environments such as cloud-native applications and microservices.

4.9 Datadog

Datadog specializes in providing a comprehensive monitoring platform for cloud applications. It collects data from diverse sources such as servers, containers, databases, and third-party services. By offering these features, Datadog assists DevOps teams in preventing downtime, addressing performance problems, and ensuring optimal user experience.

4.10 CA Application Performance Management (CA APM)

CA Application Performance Management is a tool for real-time application monitoring, designed to help organizations manage and optimize application performance. It offers a full view of application health, providing insights into infrastructure, network performance, and end-user experience. CA APM's real-time diagnostics enable IT teams to quickly address performance issues, improving overall system efficiency and user satisfaction.

4.11 DX Application Performance Management (DX APM)

DX Application Performance Management is an advanced application performance management tool that helps organizations monitor the performance of their applications and optimize user experiences. It provides proactive monitoring, real-time insights, and detailed root cause analysis. DX APM helps IT teams identify performance problems before they impact users and enables end-to-end visibility of application transactions and microservices across complex environments.

4.12 Prometheus and Grafana

Prometheus and Grafana: Prometheus is an open-source monitoring and alerting toolkit designed for capturing time-series data, particularly in cloud-native and microservices environments. When combined with Grafana, a popular visualization tool, it offers powerful dashboards and

Vol. 10, No. 06; 2025

ISSN: 2456-3676

real-time metrics to track application performance and infrastructure health. This combination is widely used for monitoring Kubernetes clusters and other containerized environments.

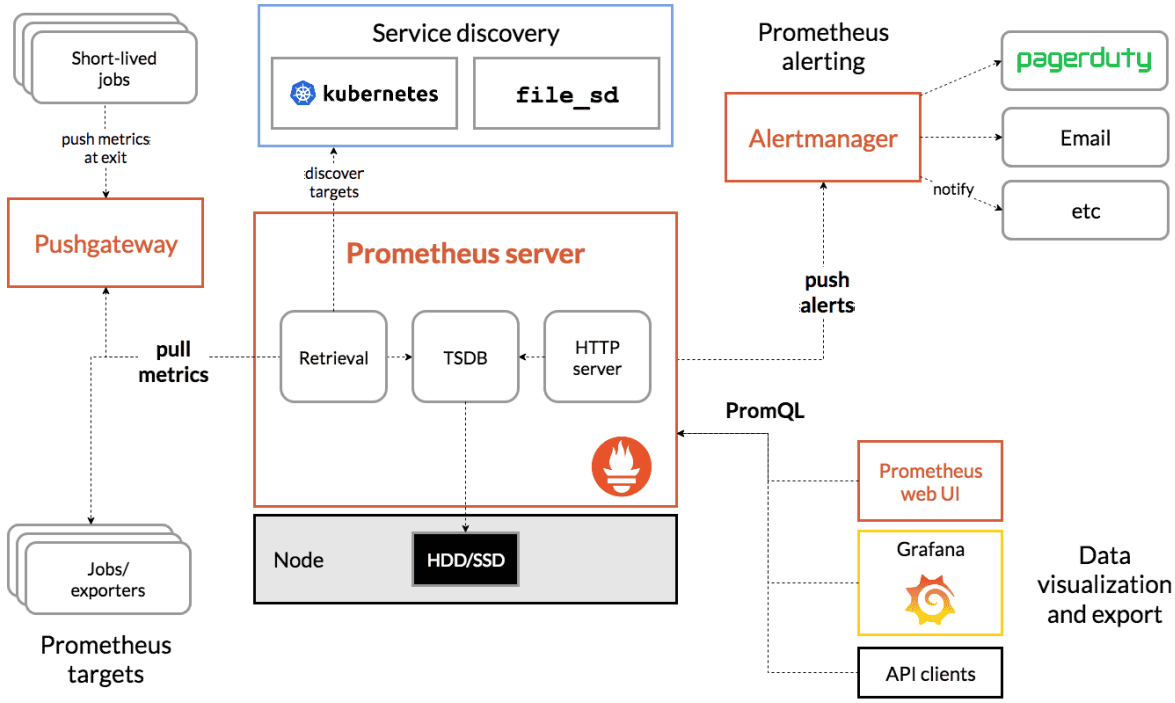

Figure 2: **Prometheus** is an open-source monitoring and alerting tool,

https://uptrace.dev/tools/monitoring-tools-for-it (accessed Feb. 20, 2025)

4.13 Nagios

Nagios is one of the most popular open-source monitoring tools designed to keep track of the health and performance of network devices, servers, and applications. It provides real-time monitoring, alerting, and reporting on the status of IT systems. Nagios is scalable, allowing organizations to monitor everything from small setups to large, distributed infrastructures. It also offers a broad range of plugins that can be used to extend its functionality.

4.14 PRTG Network Monitor

PRTG Network Monitor is a comprehensive monitoring tool designed to monitor various aspects of IT infrastructure. It is used to track the performance and availability of networks, servers, applications, and IT infrastructure. PRTG offers real-time monitoring with customizable alerts and notifications, ensuring that potential issues are identified and addressed before they cause disruptions. The tool is easy to set up and use, making it a popular choice for organizations of all sizes. Its ability to monitor a wide range of systems and devices makes it a versatile solution for network and infrastructure management.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

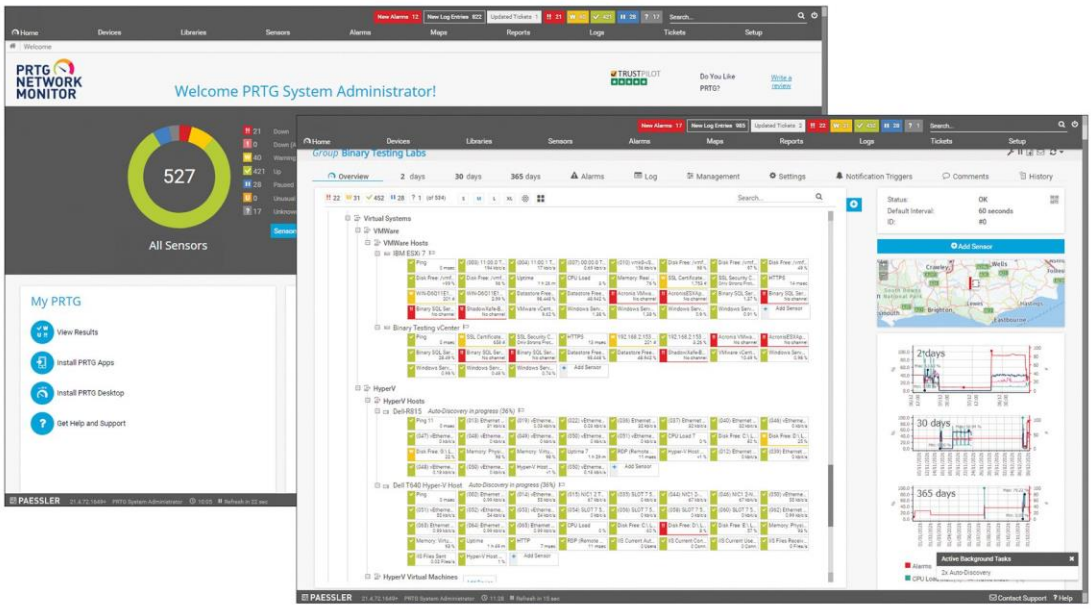

Figure 3: **PRTG** is a network monitoring tool,

https://uptrace.dev/tools/monitoring-tools-for-it (accessed Feb. 20, 2025)

4.15 Comparative evaluation of monitoring systems

In contemporary enterprise environments, monitoring and security information and event management (SIEM) platforms are indispensable for ensuring operational resilience, performance optimization, and regulatory compliance. The systems under consideration—PRTG, Nagios, Zabbix, Prometheus with Grafana, DX (CA) Application Performance Management, Datadog, Dynatrace, McAfee Enterprise Security Manager, Rapid7 InsightIDR, LogRhythm, IBM QRadar, Splunk, and Azure Sentinel—represent distinct traditions within infrastructure monitoring, application performance management, and security analytics. A critical comparative evaluation reveals both convergences and divergences in their scalability, analytical depth, and suitability for hybrid cloud and regulated financial environments.

Infrastructure monitoring solutions such as PRTG, Nagios, Zabbix, and Prometheus with Grafana embody different paradigms of visibility. PRTG emphasizes ease of deployment through sensor-based monitoring, offering rapid insight into heterogeneous infrastructures but at the cost of licensing complexity in large estates. Nagios, by contrast, remains rooted in a plugin-driven model that provides high flexibility and scriptability, yet demands significant manual configuration and struggles with scalability in dynamic environments. Zabbix advances a more integrated approach, combining agent-based and agentless monitoring with strong templating, making it attractive for cost-sensitive enterprises, though its management overhead grows with scale. Prometheus and Grafana, meanwhile, epitomize the cloud-native ethos: Prometheus's

Vol. 10, No. 06; 2025

ISSN: 2456-3676

time-series database and pull-based scraping model align seamlessly with Kubernetes and microservices, while Grafana delivers powerful visualization. Their limitation lies in the need for complementary tools to handle logs and traces, underscoring the modularity of cloud-native observability stacks.

Application performance management platforms extend monitoring into the domain of distributed tracing and user experience. DX (CA) APM reflects a legacy enterprise orientation, excelling in baseline analysis of monolithic applications but offering limited agility in cloud-native contexts. Datadog, as a SaaS-based observability platform, integrates infrastructure, APM, logs, and synthetic monitoring into a unified service, enabling rapid deployment and broad integration. Its usage-based pricing, however, introduces volatility in total cost of ownership. Dynatrace distinguishes itself through its OneAgent architecture and Davis AI engine, which provide automated topology discovery and anomaly detection across complex distributed systems. While its analytical sophistication is unmatched, its premium licensing and vendor lock-in risks require careful governance. Collectively, these APM platforms illustrate the tension between legacy enterprise stability and modern cloud-native adaptability.

The SIEM and security analytics platforms McAfee Enterprise Security Manager, Rapid7 InsightIDR, LogRhythm, IBM QRadar, Splunk, and Azure Sentinel address the imperative of threat detection, compliance, and incident response. McAfee ESM remains anchored in endpoint-centric SIEM traditions, offering solid event correlation but limited cloud-native integration. Rapid7 InsightIDR emphasizes user and entity behavior analytics (UEBA) within a SaaS delivery model, making it particularly suitable for lean security operations centres, though its extensibility is narrower than that of larger competitors. LogRhythm balances SIEM and SOAR capabilities, providing playbooks and automation for mid-sized enterprises, yet requires tuning to scale effectively. IBM QRadar excels in efficient event per second (EPS) handling and robust correlation rules, proving its value in large, regulated environments, though it is less agile in handling high-cardinality data. Splunk, by contrast, offers unparalleled flexibility in ingesting and analyzing diverse data sources, supported by a vast ecosystem and strong SOAR capabilities; its challenge lies in cost escalation without disciplined data management. Azure Sentinel represents the cloud-native evolution of SIEM, tightly integrated with Microsoft 365 and Azure signals, delivering elastic scalability and cost efficiency when paired with rigorous data hygiene. Its Azure-centricity, however, necessitates deliberate integration in multi-cloud contexts.

Taken together, these platforms illustrate a spectrum of trade-offs. Infrastructure monitoring tools range from traditional, scriptable solutions to cloud-native observability stacks, each with distinct implications for scalability and cost. APM platforms highlight the divergence between legacy enterprise baselining and modern AI-driven analytics. SIEM solutions reveal the balance between traditional on-premises correlation engines and cloud-native, elastic analytics ecosystems. For financial institutions and other regulated enterprises, the optimal choice depends on strategic priorities: whether the emphasis lies on legacy application stability, cloud-native agility, or investigative flexibility. Ultimately, the comparative analysis underscores that no

Vol. 10, No. 06; 2025

ISSN: 2456-3676

single platform suffices across all dimensions; rather, a layered architecture that combines cost-effective infrastructure monitoring, sophisticated APM, and a SIEM aligned with regulatory and cloud strategy offers the most resilient path forward.

4.16 Comparison table for Monitoring Tools

The following table presents a detailed comparison of selected monitoring tools, including their operation system compatibility and best-use scenarios.

Nr.	Monitoring Tools Name	OS Support	Best-use Scenario
1	Zabbix	Windows + Linux	Enterprise server environments
2	Prometheus + Grafana	Linux + Exporters	Cloud-native, Kubernetes monitoring
3	Datadog	Windows + Linux	Full-stack SaaS observability
4	Nagios XI	Windows + Linux	Legacy + custom plugin checks
5	PRTG Network Monitor	Windows + Linux	Mid-size network monitoring
6	IBM Qradar	Windows + Linux	Strong offence/defence analytics
7	Netdata	Windows + Linux	Real-time resource stats
8	Rapid7 InsightIDR	Windows + Linux	Full-stack SaaS observability
9	McAfee ESM	Windows + Linux	SIEM, On-Prem oriented
10	DX/CA APM	Windows + Linux	Enterprise apps
11	Dynatrace	Windows + Linux	Deep cloud-native, Full-stack SaaS
12	LogRhythm	Windows + Linux	Siem+Soar, On-Prem - Hybrid
13	Splunk	Windows + Linux	Enterprise, High-cardinality search and analytics
14	Azure Sentinel	Windows + Linux	Cloud SIEM + SOAR, Azure-first

Figure 4: **Table** of monitoring tools, *Complied by the Author (Nov. 29, 2025)*

Vol. 10, No. 06; 2025

ISSN: 2456-3676

5. SIEM Solutions Addressing Cybersecurity Risks

Cybersecurity risks targeting industrial control systems (ICS) have grown significantly in recent years, driven primarily by increasing activity from nation-states and cybercriminals. These attackers have become more advanced, making it more difficult to detect and respond to incidents in a timely manner. Cybersecurity threats impacting both information technology and industrial control technology (ICT) now include a wide range of attack vectors such as ransomware, malware that disrupts utility operations, phishing campaigns aimed at executives and other privileged personnel, business email compromise, data theft, and social engineering aimed at extracting sensitive information from employees.

To counter these evolving threats, cybersecurity solutions for ICS need to incorporate real-time behavioral anomaly detection, expedite incident response, and provide intelligent visualizations of interconnected networks. Security Information and Event Management systems are designed to address these needs by collecting, aggregating, storing, and correlating event data from various sources within an infrastructure. These systems play a crucial role in modern security operations centres (SOCs) by gathering events from diverse sensors, such as intrusion detection systems, firewalls, and antivirus software, and then correlating those events to provide a comprehensive view of potential threats. By doing so, SIEMs help security teams detect, manage, and report on security incidents effectively.

However, there are notable differences among the various SIEM solutions available in the market, with each offering different capabilities, strengths, and weaknesses. These differences are often a reflection of the varying positions of SIEMs in the market. Some solutions come from established IT companies, such as IBM, McAfee, and HP, while others are offered by more forward-thinking companies like AlienVault or Splunk, which are introducing innovative features that cater to the complex needs of modern cybersecurity.

SIEM systems are typically made up of several interconnected components, including event collection, log parsing and normalization, rule engines, log storage, and event monitoring. These components need to work together seamlessly for the SIEM to function properly. While many SIEM solutions now offer automated response capabilities that allow for the selection and deployment of security measures, these features are often limited in their ability to perform comprehensive impact analysis of attacks and response actions.

Overall, SIEM systems continue to evolve in response to the growing sophistication of cybersecurity threats. They are an essential tool for detecting and responding to incidents in real-time, providing vital insights into network activities, and helping security teams maintain a proactive security posture. As the landscape of cybersecurity threats continues to evolve, so too must SIEM solutions, with an ongoing focus on enhancing automation, improving data analytics, and refining response capabilities to better handle emerging risks.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

6. SIEM Features and Capabilities

SIEM systems are essential tools for organizations to collect, store, and analyze security events generated by their IT infrastructure. While all SIEMs share these fundamental capabilities, they differ significantly in terms of features, performance, and implementation. These differences are often a reflection of the systems' positions in the market, ranging from basic solutions designed for small-scale deployments to advanced systems used by large enterprises with complex security needs. When evaluating SIEM solutions, it's important to consider a variety of features that impact their effectiveness in detecting and responding to security incidents.

A key feature of any SIEM is its ability to correlate events. Correlation rules form the backbone of a SIEM's event detection capabilities, as they define how events from different sources are analyzed and linked to identify potential security incidents. While most SIEMs offer basic correlation rules, more advanced systems support complex search processing languages that allow security analysts to write sophisticated queries and conduct deeper analyses of the data. These systems are capable of handling a broader range of events and are more effective in identifying subtle patterns of malicious activity.

The ability to collect data from a wide variety of sources is another crucial aspect of a SIEM. Security events can originate from many different parts of an IT infrastructure, such as servers, firewalls, intrusion detection systems, and endpoint devices. A SIEM's effectiveness largely depends on how well it can collect data from these diverse sources. Many SIEMs natively support multiple data sources, including various sensors and data types like threat intelligence feeds. However, some solutions may require additional components or integrations to collect data from all desired sources, which can complicate the deployment and increase the overall cost. Real-time data processing is another vital feature of SIEM systems, as the security landscape is constantly evolving. The ability to process and analyze data in real-time enables SIEMs to detect and respond to threats as they occur, rather than after the fact. This requires significant computational power, as SIEMs must handle millions of events per second without compromising performance. Advanced SIEMs can provide real-time monitoring and alerting, ensuring that security teams can quickly identify and mitigate security incidents.

Handling large volumes of data is also a critical challenge for SIEM solutions. As organizations grow and deploy more devices and sensors, the amount of data generated increases exponentially. While analyzing large datasets can provide valuable insights into security events, it can be costly and impractical to store all collected data indefinitely. Therefore, many SIEMs are designed to support large volumes of data for short periods, with a focus on efficient indexing, correlation, and storage. This allows security teams to maintain visibility into past events without overwhelming their storage resources.

Data visualization is often an overlooked feature in SIEM systems, but it is crucial for effective security event analysis. Many SIEMs lack robust visualization tools, making it difficult for analysts to interact with and explore collected data. To address this, more advanced solutions

Vol. 10, No. 06; 2025

ISSN: 2456-3676

provide customizable dashboards and visualizations that allow security teams to better understand and interpret security events. These features can improve decision-making and help teams identify trends or emerging threats more easily.

In recent years, the integration of advanced data analytics into SIEMs has become a major trend. Modern SIEM systems can integrate with anomaly detection tools that analyze the behavior of users and applications, looking for signs of suspicious or malicious activity. These systems can use machine learning and artificial intelligence to detect unusual patterns, such as an employee accessing sensitive data they normally wouldn't or a third-party contractor attempting to exploit vulnerabilities. This type of behavior analytics enhances the SIEM's ability to detect threats that might not be identified through traditional rule-based approaches.

Performance is another key consideration when evaluating SIEM solutions. A SIEM must be able to handle the computational demands of processing large amounts of data, correlating events, and storing information for future analysis. High-performance systems are capable of managing these tasks efficiently, with fast data processing, robust storage capabilities, and the ability to scale as the organization's infrastructure grows.

Forensics is another critical feature for some SIEMs. In addition to event logging, some systems offer built-in forensic capabilities, such as network session captures. These tools allow security teams to go beyond event logs and reconstruct malicious activities, such as replaying network traffic to understand the full scope of an attack. Not all SIEMs have this capability, and the level of forensic detail provided can vary greatly across different solutions.

Deployment complexity is an important factor when choosing a SIEM solution. While some systems are relatively easy to install and manage, others require a significant amount of effort to configure and maintain. The complexity of deployment can vary depending on the features and scalability of the system, as well as the support provided by the vendor. Systems like ArcSight, for instance, are known for being difficult to deploy and manage, while others like LogRhythm and Splunk are often praised for their user-friendly interfaces and simpler setup processes.

Scalability is another key feature to consider. As organizations grow, so too do their security needs. A SIEM must be able to scale not only in terms of hardware but also in its ability to process and analyze an increasing volume of security events. This becomes particularly important in the context of digital transformation, where more devices, sensors, and endpoints are constantly being added to the network.

Risk analysis is a newer feature that has been integrated into some of the leading SIEM systems. These systems can evaluate the risk posed by various assets in the infrastructure, helping organizations identify and prioritize vulnerabilities based on their potential impact. This can be done natively within the SIEM or through integration with external tools, providing a more comprehensive approach to risk management.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

In terms of storage, SIEM systems generally retain event data for a limited time, typically up to 90 days. This feature evaluates how long SIEM solutions can store data and the efficiency with which they can manage large amounts of information over time. The longer the retention period, the more valuable the system becomes for performing forensics or compliance-related tasks.

Cost is always a factor when evaluating SIEM solutions, as the price can vary greatly depending on the features and scale of the system. Many SIEMs come with high licensing fees, but solutions like LogRhythm, USM, and SolarWinds offer more affordable options. Open-source SIEMs may also provide a cost-effective alternative, though they often come with limitations in terms of functionality and support.

Resilience and fault tolerance are important considerations, especially for critical systems like SIEMs. These systems must be able to recover from failures and continue monitoring without disruption. Features like disaster recovery, high availability, and fault-tolerant architectures ensure that the SIEM remains operational even in the event of hardware or software failures.
Finally, the ability to react to and report on security incidents is an important aspect of a SIEM. These systems should be able to automatically respond to detected threats, either by triggering alerts, activating remediation processes, or sharing information with other systems or stakeholders. Reporting capabilities also enable organizations to document incidents, track progress, and comply with regulatory requirements.

Overall, the effectiveness of a SIEM solution depends on its ability to integrate multiple features, such as data collection, real-time processing, analytics, and forensics, into a cohesive and scalable system. Choosing the right SIEM requires understanding the specific needs of an organization and evaluating how well different solutions can meet those needs.

7. Industry-Specific Challenges in Infrastructure Monitoring and Automation

In the domain of infrastructure monitoring and automation, organizations across diverse industries encounter a spectrum of complex challenges that fundamentally shape the manner in which operational environments are supervised and secured. Among these, regulatory compliance emerges as a critical determinant, given that sector-specific legal frameworks impose stringent requirements on information technology (IT) operations. Ensuring that monitoring and automation processes conform to such standards is indispensable. For instance, in the healthcare sector, regulations such as the Health Insurance Portability and Accountability Act (HIPAA) mandate the deployment of resilient monitoring architectures designed to preserve the confidentiality, integrity, and availability of patient data. Compliance in these contexts necessitates continuous, real-time surveillance coupled with automated incident response mechanisms, thereby highlighting the imperative of extending enterprise application monitoring capabilities while adhering to regulatory boundaries.

Beyond compliance, the management of sensitive data constitutes a further challenge, particularly in industries where information security is paramount. The financial sector

Vol. 10, No. 06; 2025

ISSN: 2456-3676

exemplifies this issue, as it processes extensive volumes of confidential financial information that require advanced monitoring solutions capable of generating granular insights without compromising data protection. The ability to balance robust security with effective monitoring is essential, as breaches in this equilibrium may result in severe organizational and societal consequences. Thus, examining how industries reconcile these competing demands provides valuable knowledge for the design of efficient monitoring frameworks.

Scalability represents another dimension of complexity, especially for rapidly expanding sectors such as e-commerce and online services. In these environments, monitoring infrastructures must be capable of horizontal scaling to accommodate increasing user populations and transaction volumes. Automation plays a pivotal role in this process, enabling dynamic resource provisioning, performance optimization, and the adaptive evolution of monitoring systems in alignment with organizational growth trajectories. Addressing scalability challenges yields critical insights for enterprises seeking to strengthen their monitoring and automation capacities in parallel with expansion.

Finally, technological fragmentation persists as a structural obstacle, particularly in manufacturing contexts where operational technology (OT) and IT systems coexist. The heterogeneity of these environments necessitates adaptive monitoring solutions capable of integrating across disparate technological domains. Bridging the divide between OT and IT systems facilitates a holistic perspective of organizational infrastructure, while automation must be sufficiently versatile to manage incidents across diverse technology stacks. Overcoming fragmentation is therefore essential for enabling automated diagnostics and remediation, ultimately fostering a unified and efficient approach to monitoring within complex technological landscapes.

8. The Strategic Role of Artificial Intelligence in Advancing Cybersecurity Frameworks

Artificial intelligence and machine learning have become indispensable components of contemporary cybersecurity, particularly as digital threats grow in complexity and sophistication. While these technologies provide substantial opportunities—ranging from anomaly detection to natural language processing—they cannot be regarded as universal solutions. Effective cyber risk management requires the integration of AI-driven methods with established security practices, ensuring that organizations adopt a balanced, multi-layered defence strategy.

The cybersecurity landscape is increasingly pressured by the consolidation of business operations onto fewer digital platforms, which expands the interconnected attack surface. Hybrid work models and the widespread adoption of collaboration tools such as Microsoft Teams and Slack have introduced new vulnerabilities, rendering organizations more susceptible to targeted intrusions. The aggregation of large-scale data within major service providers has simultaneously elevated the attractiveness of these platforms to adversaries, thereby amplifying both the risk and potential cost of breaches.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

AI offers distinct advantages, including the rapid processing of extensive datasets, adaptive decision-making, and task automation. However, its deployment must be carefully managed. Generative AI, for example, has already been exploited to craft highly convincing phishing campaigns, intensifying the threat environment. Although the long-term implications of generative AI remain uncertain, its role in amplifying cyber risks is evident.

Decision-making in cybersecurity—whether to permit, block, or remediate specific actions—requires precision and scalability. AI can accelerate these processes, but its effectiveness is maximized only when embedded within broader defence architectures. Leading security providers increasingly employ AI to augment detection capabilities, neutralize threats, and alleviate the operational burden on human analysts. Nevertheless, human expertise remains indispensable for refining AI outputs, ensuring accuracy, and adapting to evolving adversarial tactics.

The success of AI and machine learning in cybersecurity is contingent upon the availability of high-quality data and informed oversight. Inadequate datasets or flawed development decisions can compromise outcomes, underscoring the necessity of rigorous data governance and expert validation. AI should be strategically deployed in domains characterized by large-scale data flows—such as anomaly detection—supported by continuous feedback mechanisms to enhance performance.

Ultimately, AI has already established itself as a critical element of multi-layered cybersecurity solutions, safeguarding communications, individuals, and organizational assets. Its future trajectory promises further expansion, though its full potential remains to be realized. The extent of its impact will depend not only on technological innovation but also on the strategic vision and expertise of those who harness it.

9. Conclusion

In summary, the significance of infrastructure monitoring in safeguarding critical systems is profound and cannot be overstated. As contemporary IT environments become increasingly complex and susceptible to evolving cybersecurity threats, the deployment of advanced monitoring tools has become indispensable. This study has examined the progression of monitoring technologies, underscoring their essential role in enhancing system performance, strengthening security, and ensuring operational reliability.

Looking ahead, Security Information and Event Management platforms are expected to advance into more sophisticated solutions. Future iterations will likely incorporate enhanced analytical capabilities, leveraging Artificial Intelligence to deliver real-time threat intelligence and predictive insights. With the escalating demand to process vast datasets efficiently, SIEM systems will prioritize scalability, adaptability, and automation, positioning themselves as critical instruments for managing dynamic cybersecurity landscapes.

Vol. 10, No. 06; 2025

ISSN: 2456-3676

Moreover, the influence of Artificial Intelligence in cybersecurity will continue to expand, transforming organizational approaches to protecting critical infrastructures. AI will augment the detection of anomalies and threats that conventional systems may fail to identify, offering unprecedented speed and precision in breach prevention. As AI and Machine Learning technologies evolve, their contributions will extend beyond monitoring to encompass risk assessment, automated response, and strategic decision-making.

By integrating the advancements of SIEM platforms with the transformative potential of AI-driven technologies, organizations can proactively mitigate emerging risks, enhance resilience, and preserve the integrity of critical infrastructures. These innovations will remain central to the future of cybersecurity, guiding industries toward more secure, adaptive, and efficient digital ecosystems.

References

Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Applied Artificial Intelligence, 38(1), e2439609. http://dx.doi.org/10.1080/08839514.2024.2439609

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67, 6969–7055. http://dx.doi.org/10.1007/s10115-025-02429-y

Eze, C. S., & Shamir, L. (2024). Analysis and Prevention of AI-Based Phishing Email Attacks. Electronics, 13(10), 1839. http://dx.doi.org/10.3390/electronics13101839

Uptrace. (n.d.). What is infrastructure monitoring? Retrieved March 22, 2025, from https://uptrace.dev/glossary/what-is-infrastructure-monitoring

Uptrace. (2025, March 20). Best DataDog competitors in 2025. Retrieved March 20, 2025, from https://uptrace.dev/blog/datadog-competitors

SentinelOne. (n.d.). Emerging trends in cybersecurity monitoring. Retrieved November 23, 2025, from https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber- security-monitoring

NiCE IT Management Solutions GmbH. (2024, March). Navigating industry-specific challenges in infrastructure monitoring and automation. White Paper. Retrieved November 15, 2025, from https://www.nice.de/wp-content/uploads/2024/03/Monitoring- and-Automation-Whitepaper-by-NiCE- 2024Q1.pdf

Uptrace. (2025, January 15). Top 11 best monitoring tools for IT infrastructure. Retrieved November 23, 2025, from https://uptrace.dev/tools/monitoring-tools-for-it

Kelly, W., & Foster, E. (2024, December 20). Compare 8 tools for IT monitoring in 2025. TechTarget. Retrieved November 11, 2025, from https://www.techtarget.com/ searchitoperations/feature/Compare-8-tools-for-IT-monitoring

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759. https://doi.org/10.3390/s21144759,

Vol. 10, No. 06; 2025

ISSN: 2456-3676

https://www.researchgate.net/publication/353214895_Security_Information_and_Event_Management_SIEM_Analysis_Trends_and_Usage_in_Critical_Infrastructures

Mimecast. (2024). AI and cybersecurity: The promise and truth of the AI security revolution. White Paper. Retrieved January 25, 2025, from https://www.mimecast.com/resources/white-papers/ai-and-cybersecurity/

Kaarrela, J. (2025). Developing a cybersecurity monitoring dashboard in Splunk. Bachelor's Thesis, Turku University of Applied Sciences. Retrieved November 6, 2025, from https://www.theseus.fi/bitstream/handle/10024/899881/Kaarrela_Jani.pdf

Muppa, N. (2023). Dynatrace setup for application performance monitoring. Journal of Artificial Intelligence, Machine Learning and Data Science, 1(2), 371–375. http://dx.doi.org/10.51219/JAIMLD/Naveen-muppa/87

Datadog. (n.d.). Infrastructure monitoring. Retrieved November 4, 2025, from https://www.datadoghq.com/product/infrastructure-monitoring/

Broadcom. (2019). DX Application Performance Management: Ensure a flawless user experience with unmatched insight and intelligence. White Paper. Retrieved October 15, 2025, from https://docs.broadcom.com/doc/dx-application-performance-management

Broadcom. (2020). CA Application Performance Management Version 10.7 Installation Guide for SAP. Retrieved October 15, 2025, from https://help.sap.com/doc/8fb326bd336f411db0e201b146ee4b3b/1.0/en-US/SAPEndUserInstructions107.pdf

Shokhin, A. (2015). Network monitoring with Zabbix. Bachelor's Thesis, Mikkeli University of Applied Sciences. Retrieved October 9, 2025, from https://www.theseus.fi/bitstream/handle/10024/94415/Bachelor_Thesis-_Anatolii_Shokhin.pdf

McAfee. (2022). Enterprise Security Manager 11.5.x Product Guide. Retrieved September 13, 2025, from https://docs.trellix.com/bundle/enterprise-security-manager-11.5.x- product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html

Rapid7. (2025). SIEM (InsightIDR) overview. Retrieved October 2, 2025, from https://docs.rapid7.com/insightidr/

LogRhythm. (2025). LogRhythm SIEM documentation. Retrieved September 5, 2025, from https://docs.logrhythm.com/lrsiem/docs/