



White Paper

White Paper by Bloor

Author Fran Howarth

September 2023

Cloud-native SIEM

*Transforming security for
the modern digital landscape*



This white paper is aimed at security operations personnel and those that oversee planning and budgeting for security in organizations of any size. It explains what cloud-native technology is, what it constitutes, and the benefits that organizations implementing it will achieve.

Executive summary

Today, almost every organization is reliant on technology, but technology is evolving fast. New developments enable organizations to achieve their goals of innovation to increase competitiveness and improve business outcomes.

But adversaries are in lockstep, looking to exploit new technologies for their nefarious deeds. New technologies are in many cases delivered via the cloud, which increases the available attack surface and threat vectors.

When tackling the threats that they face, organizations have traditionally faced enormous complexity in implementing, managing and maintaining technologies for threat investigation, detection and response, which is an increasing need for all.

Security and information event management (SIEM) systems that are built with a cloud-native architecture and delivered as a software-as-a-service (SaaS) model, are a game changer for security operations. Managed and maintained by a technology provider, they are much faster to implement and manage and can ingest feeds from numerous, disparate security controls to provide clear visibility into threats and vulnerabilities affecting the entire environment, along with automated guidance regarding remediation. Cloud-native SIEMs are beneficial to any organization because security teams can focus on the work that matters – improving threat investigation, detection and response capabilities.

This white paper is aimed at security operations personnel and those that oversee planning and budgeting for security in organizations of any size. It explains what cloud-native technology is, what it constitutes, and the benefits that organizations implementing it will achieve.

Fast facts

- Many factors are leading to an expansion in the use of cloud services, including the ongoing drive to achieve digital transformation.
- Cloud-native platforms delivered in a SaaS model are a game changer for organizations operating in hybrid environments.
- Cloud-native SIEMs can ingest massive amounts of telemetry and provide the contextualised information necessary for effective threat detection and response in today's hybrid environments.
- To be effective, the platform must offer a wide range of integrations with complementary security controls.
- Cloud-native SIEMs offer a wide range of benefits, including enhanced visibility across the technology estate whilst reducing complexity.

The bottom line

The modern security landscape is complex and requires that organizations are proactive in their protection, actively searching for threats and remediating them in an effective manner. Cloud-native SIEM platforms that are tightly integrated with other security controls will provide them with a high level of protection across hybrid environments that span on-premises systems and multiple cloud services. They will transform the security capabilities of any organization operating in today's modern digital environment.

“Cloud-native SIEMs are beneficial to any organization because security teams can focus on the work that matters – improving threat investigation, detection and response capabilities.”

Cloud usage is expanding fast

Despite initial slow growth, use of cloud applications and services has soared. Security concerns have been largely assuaged, with many now seeing cloud applications as being more secure than those deployed in-house. Another factor that has driven up usage is the rise in working from home and the need to reach remote employees and ensure that they have the tools that they need to remain productive. Ease of connectivity is proving to be a real bonus for remote employees. According to Tabscanner, global spending on public cloud services will continue to increase, growing by an expected 25% by the end of 2023 compared to the previous year.

Digital transformation initiatives are also driving the move to the cloud as organizations look to take advantage of the opportunities and benefits that the use of innovative technologies enable. According to Pluralsight, 70% of organizations have more than half of their infrastructure in the cloud and 65% operate in a multi-cloud environment. According to G2, 85% of organizations will have adopted a cloud-first strategy by 2025.

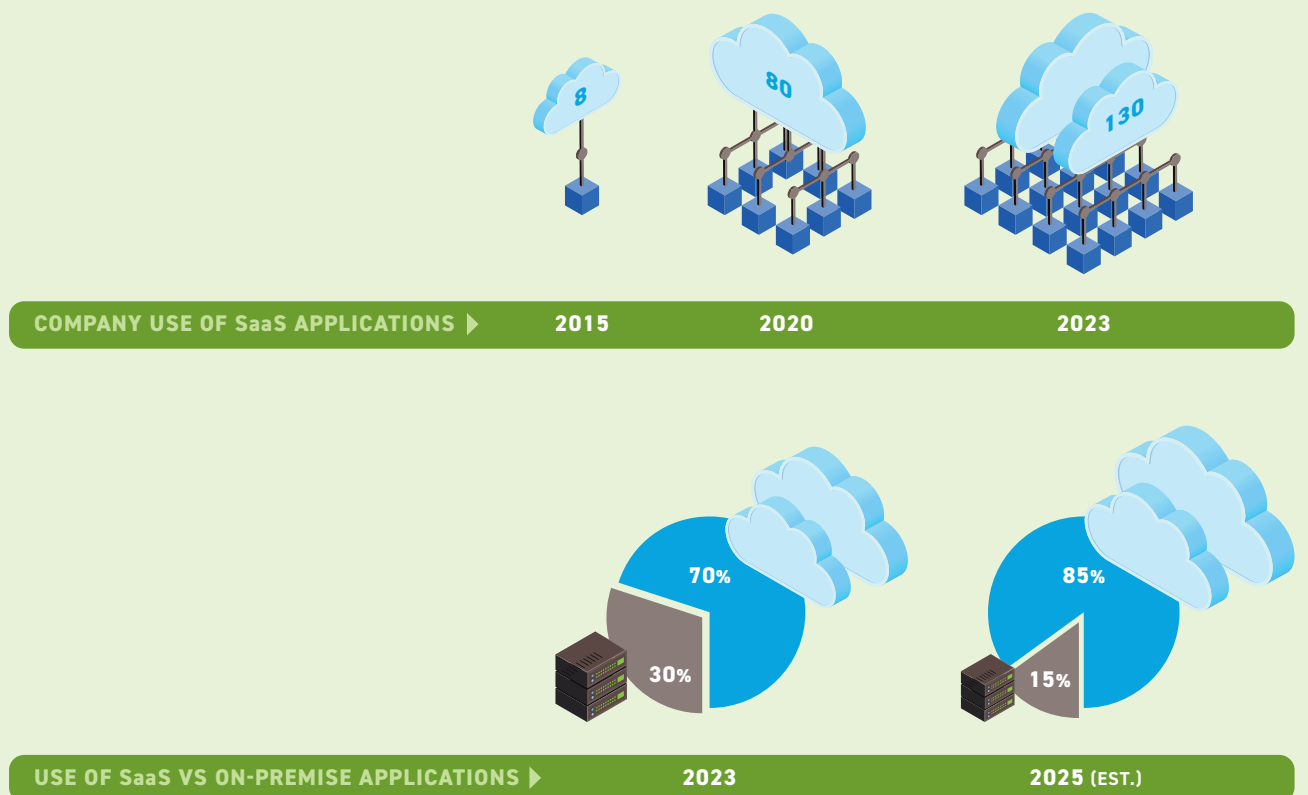
In particular, the use of SaaS applications is increasing rapidly. According to BetterCloud, organizations are using an average of 130 SaaS applications in 2023, up from 80 in 2020, and compared to just eight in 2015. SaaS applications now account for 70% of all software used by organizations and this is expected to expand to 85% by 2025.

Another driver for the growth in cloud usage is the increased importance of DevOps to improve the speed of

software delivery, bringing together all the stakeholders involved in a project, including developers, testers, operations staff and business users as a coherent team. According to Dynatrace, 94% of organizations say that DevOps that feature security tools is key to accelerating their digital transformation initiatives.

Despite these drivers, moving to the cloud is a complex matter owing to all the moving parts that are involved. Many organizations still use legacy technologies for day-to-day operations, which are difficult to implement and manage. Many applications are not suited for migration to modern servers and must be rewritten or updated before they can work properly. As a result, many are running on out-of-date servers, which creates security risks.

The complexity of modern cloud environments is high owing to the need for security, application modernization, control of sprawling infrastructure, acceleration of software delivery, the need for compliance and many more factors. According to NetApp, this complexity has reached a tipping point as 98% of organizations report that their business has been impacted by increased complexity owing to increased cybersecurity needs and risks, lack of visibility into business operations and staff burnout. Technical challenges that exacerbate complexity include the need for data mobility across clouds, alongside organizational challenges such as cost management, lack of a clear cloud strategy and leadership buy-in.



Cloud-native versus on-premises SIEM

Over the years, many traditional enterprise applications have been cloud-enabled. To do so, legacy applications must be modified to migrate the application to cloud servers so that the application can be accessed via a browser. Such applications tend to retain their monolithic structures and often lack flexibility, resiliency and scalability.

Cloud-native applications and platforms, on the other hand, are built from the ground up to be directly delivered from the cloud, providing the flexibility, resiliency and scalability that is required in the cloud. They are built using multiple small, interdependent microservices, rather than traditional applications that tend to be written as a single block structure. Microservices enable a more agile approach to development since they work independently and take minimal computing resources to run. Cloud-native applications can also be updated regularly without disrupting the service to provide additional features for meeting customer demands.

Cloud-native applications offer a host of benefits over traditional or cloud-enabled applications. They help organizations increase efficiency by enabling agile practices such as DevOps and continuous delivery. In building them, developers use automated tools, cloud services and modern design structures to ensure that they can be scaled rapidly.

They can be adopted more easily since organizations do not need to procure physical infrastructure and software that needs to be implemented before the technology can be used. Nor do they need the time that is required to manage and maintain the platform since those services are provided by the vendor.

Cloud-native technology enables resiliency to be built in to ensure availability. This means that cloud-native applications will not cause downtime. Further, they can be scaled up as needed to meet peaks in demand.

“...legacy applications must be modified to migrate the application to cloud servers so that the application can be accessed via a browser. Such applications tend to retain their monolithic structures and often lack flexibility, resiliency and scalability.”

A new era for SIEM systems

SIEM systems are seen as foundational technologies for many organizations. It is estimated that more than a quarter of all organizations have invested in a SIEM, with roughly the same amount set to do so in the near future.

SIEMs collect logs from various sources that include network devices, databases, applications and user activity into one common interface. The data collected is then analyzed, looking for any potential threats. SIEMs have long been central to threat detection efforts for many organizations, helping to guard against malware, ransomware, phishing attacks, denial of service exploits and more. They have also long been used to help organizations enhance their security posture and meet compliance objectives.

Traditionally, SIEMs have required much customization, as well as ongoing administration and management. SIEMs have also long been plagued by too many alerts, many of which are false positives, which is a burden on overstretched security teams. They were also limited in terms of the sources of data that they could ingest, were largely ineffective at cloud monitoring and struggled to detect emerging threats that had not previously been seen.

Today, leading SIEM vendors have solved many of these problems – LogRhythm's cloud security solution is a case in point. With a 20-year heritage in the SIEM space, LogRhythm Axon is an entirely new product that was built from the ground up as a cloud-native SIEM, developed with a cloud-native architecture and delivered via a SaaS model.

Cloud-native SIEMs provide easier scalability and flexibility for threat investigation, detection and response, designed to be able to ingest massive amounts of telemetry and provide contextualised analysis across huge sets of data. This includes data ingested from any cloud source through APIs, web collectors and agents, as well as on-premises applications to aid organizations working in a hybrid environment.

LogRhythm Axon is optimized for security analysts, providing automated visibility into all parts of the environment via an intuitive browser interface, allowing them to easily identify, analyze and remediate potential threats to the organization. Contextual information is easily displayed in the platform and a variety of out-of-the-box rules as well as custom rules are offered by the service. Security operations teams can leverage LogRhythm Axon to automate team workflows through case management. Case management enables analysts to automatically create cases that enable investigative workflows to track responses to threats, thus mitigating duplication of efforts and optimizing threat mitigation strategies. In addition, LogRhythm Axon enables SOC teams to test analytics rules to ensure detections are optimized for their environment.

“Cloud-native SIEMs provide easier scalability and flexibility for threat investigation, detection and response, designed to be able to ingest massive amounts of telemetry and provide contextualised analysis across huge sets of data.”

Integration with other security controls is essential

For this to be effective, integrations and complementary capabilities are essential. A SIEM system benefits from integrations to ensure that all logging data is available from all systems being monitored so that there are no gaps in protection. Log management is a fundamental capability for SIEM systems. Event correlation is another core capability of SIEMs for uncovering patterns and relationships that might otherwise not be noticed and provides additional context regarding activity. This reduces the number of false positives that must be dealt with and improves productivity.

In terms of complementary capabilities, organizations should look for several things. A platform that offers user and entity behavioural analytics (UEBA) will be able to provide the contextual security information that is required for better decision making and that offers machine learning for predictive analysis. Strong analytics capabilities are essential for effective threat detection. UEBA uses machine learning to quickly identify anomalies and threats in activity seen.

Security orchestration, automation and response (SOAR) capabilities will help in determining the steps to take for effective remediation of threats uncovered. SOAR capabilities are necessary for automating incident response where it is suitable and most offer playbooks that can guide analysts through the steps required for responding to common security threats such as ransomware.

Network detection and response (NDR) will help organizations to uncover suspicious activity within network traffic that both traverses the network laterally as well as traffic that flows into and out of the network. The monitoring performed by NDR provides real time information regarding the latest threats. Endpoint detection and response (EDR) performs similar monitoring functions, but is based on information collected by endpoints attached to the network. Taken together, NDR and EDR form the basis of extended detection and response (XDR) capabilities that provide key information regarding threats on the network.

Other integrations or native capabilities to look for include intrusion detection and response, firewalls, threat intelligence and regulatory compliance automation. Identity and access management capabilities are especially important since a very high proportion of breaches begin with the search for user credentials that can be compromised. Through effective integrations, organizations will not only gain increased visibility into security events, but also into their overall security posture, and will also be able to improve incident response times.

“Through effective integrations, organizations will not only gain increased visibility into security events, but also into their overall security posture, and will also be able to improve incident response times.”

The benefits of cloud-native SIEM

Cloud-native SIEMs provide a number of important benefits that will help organizations to achieve not only their security, but also business goals.

They are fast and intuitive to deploy and ingest all required data, compared to the implementation pains of many traditional SIEMs deployed and managed on-premises. They are easy to use and manage, since the SIEM provider performs the required tasks, and are much less complex to maintain. They are also massively scalable to meet the demands of securing any network, no matter what it encompasses.

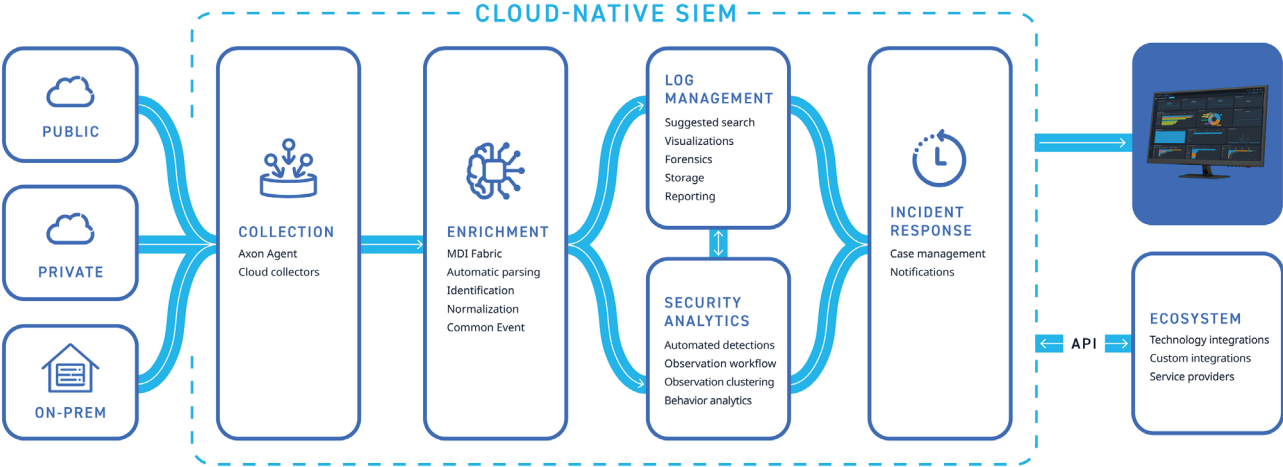
Cloud-native SIEMs provide full visibility into hybrid environments that are increasingly becoming the norm, leaving few gaps and decreasing the mean time to detect threats. Customers will benefit from the reduced time needed to protect against threats since they provide the capability to easily identify, analyze and remediate threats.

These factors mean that customers can achieve immediate value by quickly gaining insights into their security environment. Cloud-based SIEMs facilitate fast decision making and action to ensure that threats are remediated in the shortest time possible.

Making upgrades to traditional SIEMs is never an easy task, but with cloud-based SIEMs, improvements and updates to the platform are automated for every customer, further cutting down on complexity. Delivered from the cloud, enhancements can be continuously delivered without the customer needing to take any action.

LogRhythm Axon is optimized for security analysts. It has been designed so that less time is needed to train and onboard analysts, enabling them to be productive faster. This is essential considering the well-documented skills shortage in the cybersecurity industry that enables skilled professionals to pick and choose among available opportunities. Cloud-based SIEMs enables even novice analysts to work with greater efficiency and achieve better outcomes, aiding the business overall. Cloud delivery and effective, contextualized data feeds takes the strain off analysts who are provided with guided and intuitive workflows.

Metrics and reporting are provided via web-based dashboards for understanding the current security posture and for enabling organizations to improve their security maturity over time. These will also prove to be extremely valuable for achieving and proving compliance with regulatory and industry requirements.



Summary

Cloud-native applications and platforms are designed for the increasingly advanced technology that constitutes organizational networks today and into the future. In the case of SIEM systems, they are a game changer in the race to improve threat investigation, detection and response. They are a key aid for stressed analysts by providing contextual analysis of what threats are high risk and should be prioritized for remediation; furthermore, SIEMs reduce manual workload with automation throughout the workflow, helping to streamline operations and improve detection and response times. Organizations can benefit from switching to or investing in a cloud-native SIEM to meet security and compliance objectives and enable the business to successfully operate and grow in a secure manner.

About the author

FRAN HOWARTH

Practice Leader: Security



Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Bloor overview

Technology is enabling rapid business evolution. The opportunities are immense but if you do not adapt then you will not survive. So in the age of Mutable business Evolution is Essential to your success.

We'll show you the future and help you deliver it.

Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability and impact.

We provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

For over 25 years, Bloor has assisted companies to intelligently evolve: by embracing technology to adjust their strategies and achieve the best possible outcomes. At Bloor, we will help you challenge assumptions to consistently improve and succeed.

Copyright and disclaimer





This document is copyright **Bloor 2023**. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



Bloor Research International Ltd

-  20-22 Wenlock Road, London N1 7GU, United Kingdom
-  +44 (0)1494 291 992
-  info@Bloorresearch.com
-  www.Bloorresearch.com