

Organizations Embrace Advantages of Cloud SIEM

The 451 Take

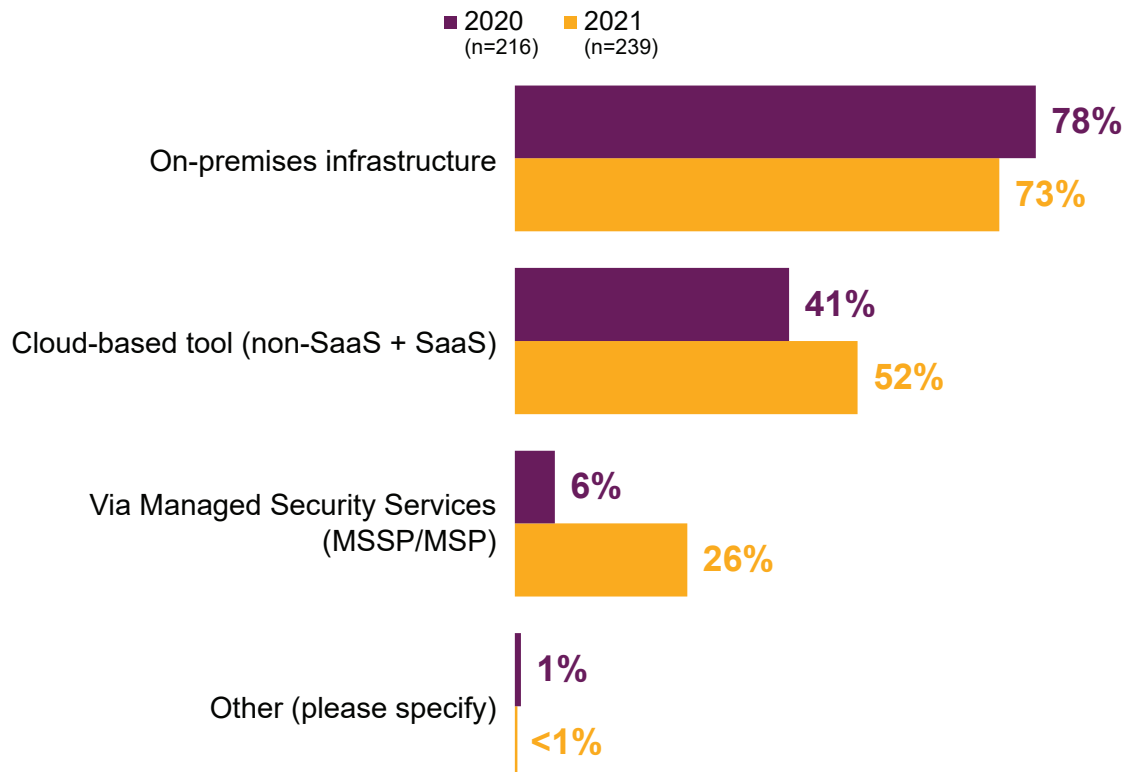
Historically, security information and event management (SIEM) has primarily been an on-premises deployment, given the need to consolidate data from enterprise tools. But because of the increased advantages of alternatives, organizational preferences for deployment models are changing – sometimes dramatically.

In successive studies published in 2020 and 2021, 451 Research's Voice of the Enterprise found that while the total number of respondents reporting on-premises deployments of SIEM had decreased, cloud deployment models and the adoption of managed security services for SIEM had both increased significantly. In 2021, the number of respondents saying they were choosing a cloud option (123) grew by 38% from 2020 (89), when they made up 41% of all survey participants versus 52% in the 2021 report. Growth among those choosing a managed services option for SIEM was even more pronounced in 2021 over 2020, by more than fourfold in percentage of each survey's respondents.

SIEM Delivery Models

Source: 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2020 and 2021

Q: How is your organization's SIEM/security analytics technology delivered? Please select all that apply.



Business Impact

CLOUD SIEM OFFERS DISTINCT OPERATIONAL ADVANTAGES TO ORGANIZATIONS. SIEM deployments are enterprise applications that have historically required an organization to invest in infrastructure and software – and more. Deployment requires expertise in best practices in this field to realize the greatest return on the investment. Organizations must maintain this investment, not only for operational, performance and system integrity reasons, but to keep it up to date with trends in the field. A cloud deployment relieves organizations of many of these burdens – and in the case of a SaaS option, functionality is ready and available for immediate use from day one.

CLOUD SIEM OFFERS SCALE AND PERFORMANCE ONLY FOUND IN A CLOUD ENVIRONMENT. The advantages of cloud map well to the value that organizations demand of SIEM. Storage in the cloud can be open-ended – good news for the availability of historical data that could indicate threats. Because cloud providers deliver availability at scale, they may be more cost-competitive for storage as well. Cloud providers may be also able to offer sophisticated analytic technologies only available to those with the resources to serve thousands of clients. These capabilities can make much more data available for more responsive analysis, enabling security teams to find evidence that might otherwise be overlooked by alternatives.

CLOUD SIEM TECHNOLOGY CAN HELP ORGANIZATIONS MAKE THE MOST OF HUMAN EXPERTISE. Security experience is scarce and dear. The priority of that expertise should, therefore, be on what only people can do – which means that organizations should focus technology on what it can do best to help alleviate demands on personnel. It's therefore not surprising that quality of reporting and alerting is the most important attribute when selecting a SIEM vendor, as reported by 74% of respondents to 451 Research's Voice of the Enterprise: Information Security, Vendor Evaluations 2021 study. Cloud SIEM can help organizations meet these needs through operations-ready deployments that deliver benefits of scale, immediacy, automation and cost.

ENTERPRISES EMBRACING THE SERVICE PROVIDER OPTION NEED SIEM THAT SUPPORTS BOTH. Organizations are significantly increasing their adoption of 'SIEM as a service,' turning to service providers to deliver SIEM capability or support SIEM with specialized expertise. Enterprises and service providers engaged in these efforts must have technology equally accessible to both – another advantage of SIEM delivered from the cloud. A cloud-based approach makes it easier for the enterprise to embrace services or adapt new capabilities to take advantage of service provider expertise quickly. For the MSSP, it reduces the total cost of operations by alleviating the service provider of many burdens of infrastructure deployment and maintenance. These, in turn, may represent cost savings they can pass along to their customers and help increase their own profitability – no small matter when access to expensive human expertise is a primary driver of service adoption.

Looking Ahead

The advantages of cloud are already contributing to drivers of changing enterprise SIEM investment, delivering value across many business priorities. In particular, the need to extend enterprise IT beyond the traditional boundaries of brick-and-mortar facilities has been accentuated in the past year, accelerated by the response to the global pandemic. These drivers won't disappear – far from it. Many organizations have indicated that a number of the remote work scenarios embraced today will persist for some time to come. The advantages of the cloud, coupled with the ability of cloud SIEM to extend security visibility and response to enterprise resources wherever they may be found, should continue to drive adoption of cloud-delivered SIEM going forward.

sumo logic®

The Sumo Logic cloud-native security information and event management (SIEM) fuses analytics and automation for security operations workflows and automatically triages security alerts. It includes advanced security analytics and correlation at scale to help organizations to efficiently and cost effectively detect and investigate security threats and attacks while helping maintain compliance requirements across cloud, hybrid, and on-premises environments. Contact [Sumo Logic](#) to experience the benefits of a cloud-native SIEM.