accelops

AccelOps
CLOUD SECURITY SURVEY 2013

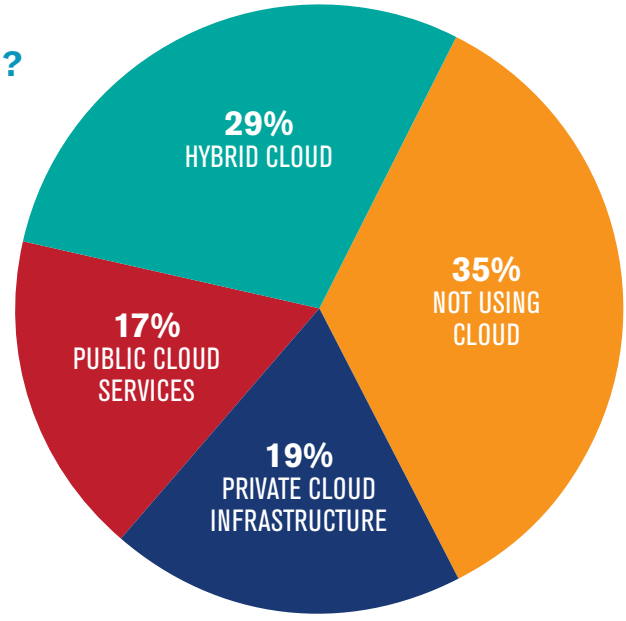
Introduction and Methodology

AccelOps, the leader in integrated Security Information and Event Management (SIEM), performance and availability monitoring software for on-premise and cloud-based data centers, conducted a survey in February 2013 to better understand how IT professionals are deploying cloud services, what issues are inhibiting security and how existing security (SIEM) and monitoring tools are meeting the challenges of cloud security.

AccelOps collected responses online and from attendees at the 2013 RSA Conference. A total of 176 IT security professionals responded. This report details the survey results and conclusions.

1. How is your organization using cloud services today for mission-critical applications and data?

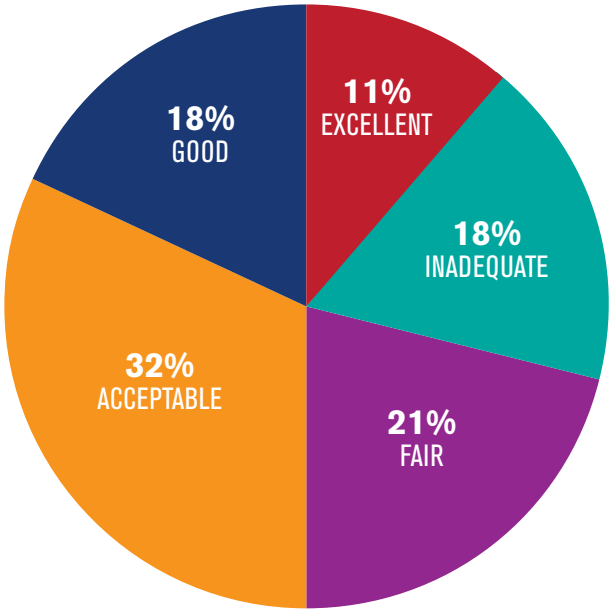
It's definitely the era of cloud services. About two-thirds, or 65 percent, of respondents said they are using some form of cloud services for mission-critical applications and data. Twenty-nine percent responded they are using hybrid clouds in their organizations. Nineteen percent have deployed a private cloud infrastructure, and 17 percent are using public cloud services. Thirty-five percent responded that they are not using any cloud services at this time.



Cloud Usage

2. How would you rate your organization's ability to ensure cloud security and regulatory compliance with your existing SIEM and infrastructure monitoring tools?

There's plenty of room for improvement here for Security Information and Event Management (SIEM) and infrastructure monitoring vendors. A total of 39 percent of respondents rate their organizations' ability to ensure cloud security and regulatory compliance using their existing SIEM and infrastructure monitoring tools as "inadequate" (18 percent) or "fair" (21 percent). Thirty-two percent rate their tools as "acceptable," and 18 and 11 percent rate them as "good" or "excellent," respectively.

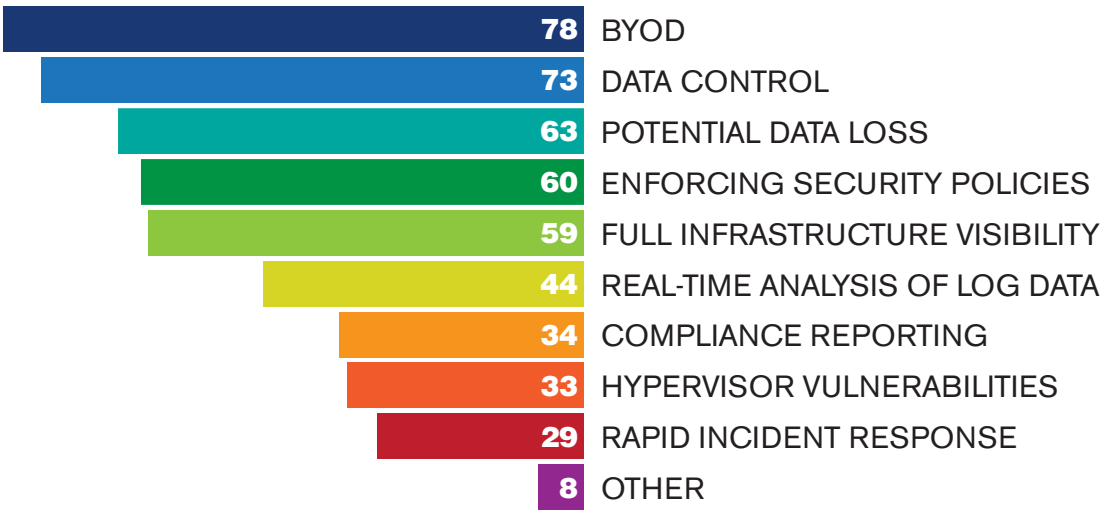


Rate Existing Cloud Security Tools

3. Please select the three issues that you think are the greatest inhibitors to effective cloud security. Choose up to three.

Bring Your Own Device (BYOD) (78 responses) and data control (73 responses) were listed as the top cloud security inhibitors, followed by potential data loss (63 responses), enforcing security policies (60 responses), and full infrastructure visibility (59 responses). Real-time analysis of log data (44 responses), compliance reporting (34 responses), hypervisor vulnerabilities (33 responses) and rapid incident response (29 responses) were also identified as significant inhibitors.

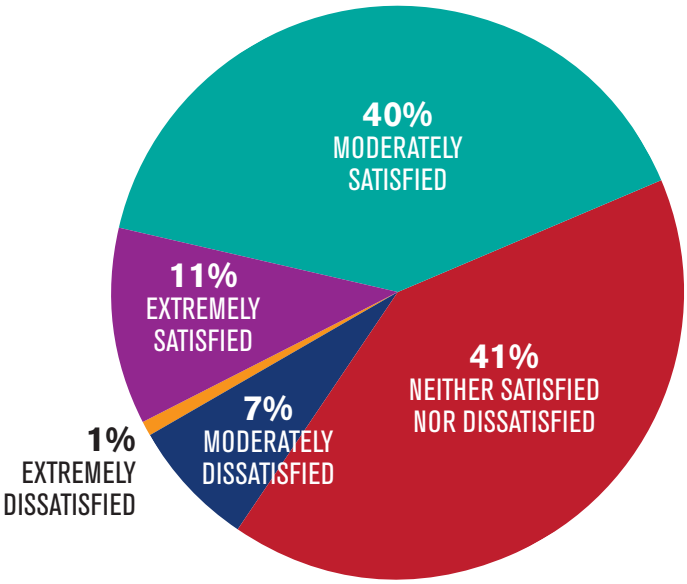
Respondents were asked to specify any non-listed concerns. There were eight such responses, which identified trust, data granularity, capacity management, correlation, government requirements and employee training as additional inhibitors to cloud security.



Cloud Security Inhibitors

4. How satisfied is your organization with the security and access control SLAs that your cloud service provider offers?

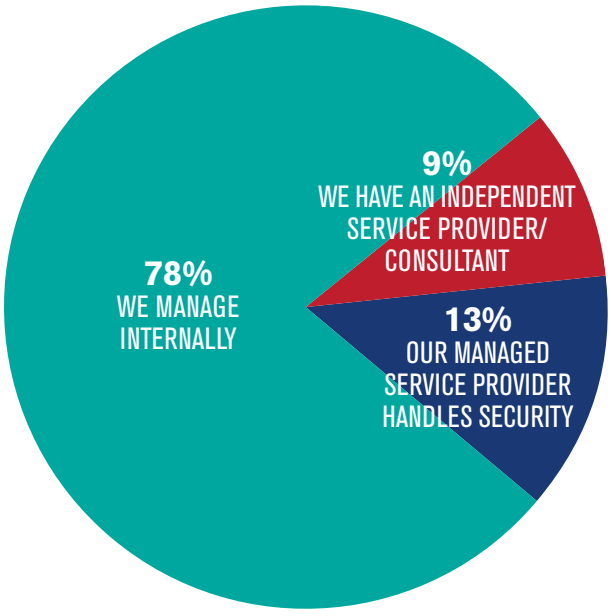
This one was close. Forty-one percent were neutral, indicating they were "neither satisfied nor dissatisfied" with the security and access control Service-Level Agreements (SLAs) provided by their cloud service providers, while 40 percent were "moderately satisfied" and 11 percent were "extremely satisfied." Only 8 percent report being "moderately" or "extremely dissatisfied."



Service Provider SLA Satisfaction

5. Who has responsibility for your organization's cloud security?

Responsibility for the data and management of cloud remains internal. Overwhelmingly, survey respondents report that their organizations are managing cloud security internally (78 percent). Thirteen percent said they use a Managed Service Provider (MSP) and only 9 percent said they utilize independent service providers or consultants. Some respondents reported that responsibility for their organizations' cloud security is shared between internal resources and external providers.



Cloud Security Responsibility

SURVEY CONCLUSIONS

Cloud security is obviously of high interest to security professionals, and no wonder with 65 percent of survey respondents saying they already rely on cloud services of some sort for their mission-critical applications and data.

Dissatisfaction with Existing SIEM Tools for the Cloud

A top concern gleaned from the survey is the 39 percent of respondents who said they could not rely on their existing SIEM and infrastructure monitoring tools for cloud security and regulatory compliance.

"It's a sad indictment of the security industry that in such a well-established market as SIEM and performance monitoring that 39 percent of those surveyed indicated that they could not rely on their existing SIEM and monitoring solutions to ensure cloud security and compliance," said Flint Brenton, AccelOps President and CEO. "Unfortunately for many organizations, they are tied into SIEM and monitoring tools designed before the advent of cloud computing and even virtualization, and well before users began bringing smartphones and tablets to the workplace."

In many instances, organizations have deployed multiple tools with specialized functionality to have visibility into discrete areas of their infrastructure, such as network devices, servers or applications.

"These siloed solutions are creating blind spots and vulnerabilities, as well as creating a management nightmare that is expensive to maintain," Brenton said.

BYOD Proves to be a Top Concern

It is not surprising that the survey reports that the number one inhibitor to effective cloud security is BYOD. It's a high priority challenge to resource-constrained IT administrators as more employees access corporate networks and data using an ever-evolving array of personal devices.

Numerous studies have shown that giving employees their choice in mobile devices improves both productivity and job satisfaction while reducing the expense to the organization. Workers use personal devices from home, on the road and on the weekend to keep up with business demands. Their personal applications and social media create an increased security risk and challenge to privacy.

BYOD brings increased risks to network security, loss of intellectual property, impact on critical business application performance and more. Increasingly, consumer-oriented services and applications such as Evernote or Dropbox that are hosted on both enterprise desktops and mobile devices represent a vulnerability to corporate data that hackers are exploiting to get access to sensitive information. This threat further compounds the already significant challenges to IT departments in ensuring security, performance and availability across the distributed IT infrastructure.

Next-generation monitoring tools are needed to track user and mobile device activity, quickly remedy security breaches and manage impacts to business application performance.

Data Control is a Close Second Priority

Also at the forefront of IT security analysts and business executives' concerns is control over corporate data once it is moved into any third-party cloud service. Organizations are fearful of having their information compromised and are reticent to allow cloud service providers any visibility into sensitive data. All the long-established security concerns applied to the enterprise must be addressed by cloud service providers. Overcoming these concerns requires that cloud service providers be transparent on how data flows through their services, who has access to the data, as well as ownership and security measures to protect the data. To alleviate these concerns, service provider agreements should include SLAs that ensure that the data is secure, always available and under the organizations' IT control.

Data control risks must be managed in cloud environments by the provider.

"The promise of cloud computing is to improve agility and deliver greater efficiencies and cost savings," Brenton said. "However, unless risk can be managed and data secured effectively, organizations will not fully benefit from the advantages of the cloud."

Data Loss Prevention is Also a Concern

With BYOD and the proliferation of IP-connected devices in the workplace, it's no great surprise that data loss prevention (DLP) is a top-of-mind issue for security professionals. Mobile devices represent a

higher-risk case for organizations because of the increased vulnerabilities that mobility and comingled enterprise and personal usage model. As a result, enterprises are struggling to establish a comprehensive strategy, policies and procedures for endpoint DLP.

The effectiveness of data discovery and classification tools and processes are a key component of DLP and data leakage solutions. Once data is properly classified, integrated security applications that monitor network traffic, storage and data center file server or database infrastructure can detect and monitor sensitive data, and alert administrators to any policy violations resulting from data sent outside the enterprise.

Cloud Security Managed Internally

It is not surprising that 78 percent of organizations, even those depending on cloud services, manage cloud security internally. Organizations must retain ownership and responsibility for their own data, irrespective of the underlying security and processes implemented by the cloud service provider.

Organizations require unified visibility, dashboards and reporting capabilities regardless of who is actually managing the infrastructure. Infrastructure security from the organizations' perspective should be seamless between their private infrastructure and the cloud so confidential data is protected no matter where it is located.

Improving Customer Satisfaction with SLAs

Forty-one percent of survey respondents said they were "neither satisfied nor dissatisfied" with the security and access control Service-Level Agreements (SLAs) provided by their cloud service providers.

"There is a clear opportunity to improve customer satisfaction with the 41 percent of survey respondents who were neutral on this issue," Brenton said. "This data supports our conclusion that it's important that technology vendors need to support MSPs with capabilities such as native multi-tenancy and the ability to provide dashboards and SLA reporting on a per-customer basis, even in shared infrastructures. Customers need a coherent solution to manage security and compliance internally, even as they move more data and applications to public cloud services."

SUMMARY

With 65 percent of survey respondents saying their organizations use the cloud for their mission-critical applications and data, of primary concern is the 39 percent who said they could not rely on their existing SIEM and infrastructure monitoring tools for cloud security and regulatory compliance.

SIEM and monitoring tools designed before the advent of cloud computing, and even before virtualization and BYOD, have resulted in organizations wasting resources on multiple, point-solution tools with specialized functionality to have visibility into discrete areas of their infrastructure, such as network devices, servers or applications.

These siloed solutions have created blind spots and vulnerabilities, as well as creating an unwieldy and costly management nightmare.

Next-generation infrastructure monitoring tools are needed to track security, performance and availability on-premise and in the cloud – all on one pane of glass. Organizations also require real-time alerts and remediation for security breaches and performance-impacting events.

Other inhibitors to cloud security reported in the survey are BYOD and concerns over control of data once it is moved into any third-party cloud service.

Cloud service providers must be transparent as to how data flows through their services, who has access to the data, as well as ownership and security measures to protect the data. Service provider agreements should include SLAs that ensure that the data is secure, always available and under the organizations' IT control.

Ultimately, organizations using the cloud are responsible for understanding and managing their risk postures and compliance capabilities, and need the tools to ensure that they can do this effectively.

How AccelOps Secures the Cloud

AccelOps' all-in-one security, performance and availability monitoring software was architected as a true infrastructure-wide solution to help organizations have a more secure and successful cloud experience.

AccelOps provides full visibility across the infrastructure – servers, storage, network and security devices, appli-

cations and users – whether on-premise or in the cloud. Its patented real-time analytics technology enables the software to make sense of behavior patterns to rapidly detect and solve problems.

The AccelOps application ensures the integrity, reliability and confidentiality of data by applying a single, unified platform to predict cloud security threats and IT operational issues using real-time analytics and event correlation. This solution provides deep contextual intelligence by appending event data with role and identity data and geo-location data that enables an open, but secure environment. AccelOps' unified security solution provides user activity monitoring, change monitoring, role-based access control and threat detection, and provides a comprehensive approach to maintain data control.

AccelOps' security software also works alongside wireless access and mobile device management vendors to eliminate vulnerabilities created by BYOD. The company continues to enhance features such as periodic discovery that dynamically detects new devices, directory service configuration changes and update the Configuration Management Database.

AccelOps supports MSPs with native multi-tenancy and the ability to provide dashboards and SLA reporting on a per-customer basis, even in shared infrastructures. By supporting MSPs in this way, this integrated security and performance monitoring platform can help them expand their revenue opportunities by enabling their customers to have a coherent solution to manage security and compliance internally even as they move more data and applications to public cloud services.

AccelOps provides organizations with an all-in-one tool that offers full visibility, dashboards and reporting capabilities regardless of who is actually managing the infrastructure.

About AccelOps

AccelOps provides a new generation of integrated security, performance and availability monitoring software for today's dynamic, virtualized data centers. Based on patented distributed real-time analytics technology, AccelOps automatically analyzes and makes sense of behavior patterns spanning server, storage, network, security, users, and applications to rapidly detect and resolve problems. AccelOps works across traditional data centers as well as private and hybrid clouds. The software-only application runs on a VMware ESX or ESXi virtual appliance and scales seamlessly by adding additional VMs to a cluster. Its unmatched delivery of real-time, proactive security and operational intelligence allows organizations to be more responsive and competitive as they expand the IT capabilities that underpin their business.

AccelOps, Inc.
2901 Tasman Drive, Suite 100
Santa Clara, CA 95054
USA

Web: www.accelops.com
Tel: 1 (408) 490-0903
Email: info@accelops.com