2018 GLOBAL SECURITY TRENDS IN THE CLOUD

A SURVEY OF IT SECURITY PROFESSIONALS

April 2018

dimensional research

Sponsored by sumologic

2018 GLOBAL SECURITY TRENDS IN THE CLOUD
A SURVEY OF IT SECURITY PROFESSIONALS

Dimensional Research | April 2018

Introduction

IT continues its dramatic evolution: application architecture has been modernized, deployment processes are being updated, and infrastructure is rapidly evolving. Within this new world of IT, there is no question that cloud adoption is happening at an aggressive rate. Security has historically been one of the biggest challenges for moving infrastructure to the cloud. Many organizations delayed their initial cloud adoption because of concerns about losing control of their environment, keeping data secure as it moved between environments, and a variety of other potential security risks. With time, however, the operational, cost, and business agility benefits of the cloud became so apparent that IT teams were compelled to figure out how to make the transition, and the adoption of cloud accelerated dramatically.

The challenge of ensuring security in cloud environments did not just disappear though. Changing technology typically requires new approaches to security, and cloud is no different. So how are development, operations and security teams adapting to the needs of the new cloud paradigm? What challenges are they facing? Are existing organizations and tools right for cloud environments or is there a need for change?

The following report, sponsored by Sumo Logic, is based on a global survey of 316 IT security professionals responsible for environments with significant investment in both cloud and on-prem infrastructure. The goal of this survey was to quantify current experiences with adopting traditional security methods in the cloud, with a focus on both organizations and tools.

In this research project, “cloud” refers to public Infrastructure-as-a-Service (IaaS) such as Amazon AWS, Microsoft Azure, and Google Cloud Platform. Survey participants were given this definition and asked to think of their IaaS environment when answering questions about cloud.

Sponsored by 

Key Findings

- **Organizations are modernizing IT infrastructures, applications and processes**
  - 76% are embracing DevOps
  - Only 16% characterize their cloud adoption as mature, with a further 59% describing themselves as in process and 25% saying they are still learning
- **Security in the cloud creates new challenges and need for collaboration**
  - 97% face organizational challenges with security in cloud environments
  - 63% say cloud requires broader technical expertise to understand threats
  - 87% report the need for multiple functions (development, security, operations, DevOps, etc.) to be involved in security threats is greater in cloud environments
  - 82% say they have more investigations which involve both application and infrastructure layers in their cloud environments
  - 93% face challenges with their security tools in cloud environments
- **Traditional on-prem SIEM solutions are not a fit for cloud**
  - 83% who use their existing on-prem SIEM in the cloud have issues including 51% who can't effectively assimilate cloud data and threats
  - Only 10% are fully satisfied with using their on-prem SIEM for the cloud

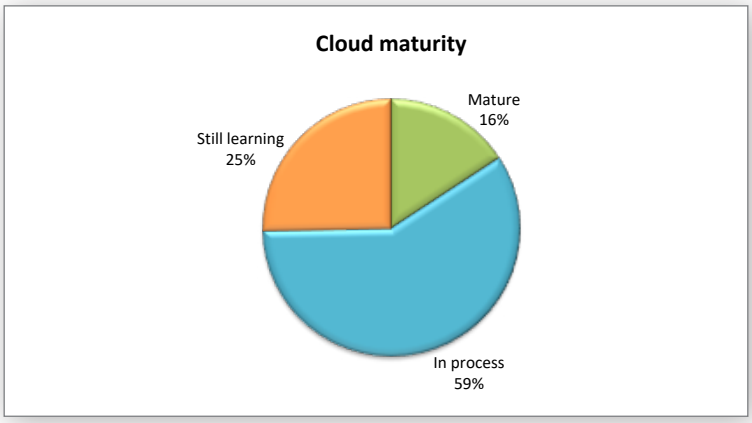
New models are needed to break down silos of people, workflow, and technology

- 95% say cloud security would benefit from organizational changes
- 96% would benefit from additional cloud security capabilities in their tools

Detailed Findings: Organizations are modernizing IT infrastructures, applications and processes

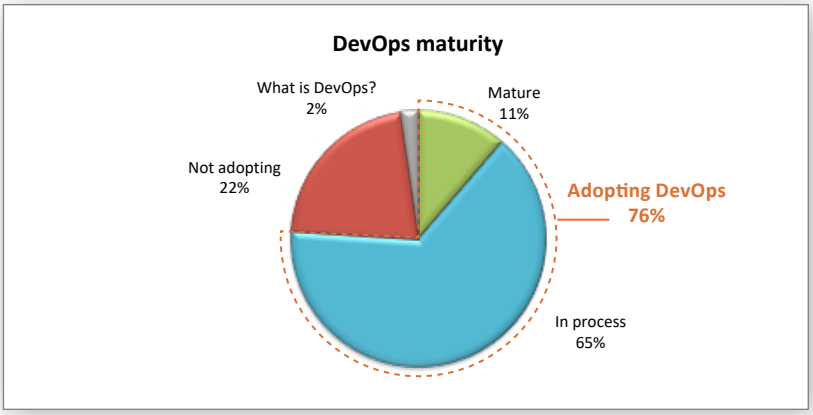
Processes and technology adoption are still evolving

All participants in this study have made a significant investment in cloud as a requirement to participate, but we wanted to know what people thought about their maturity. The clear answer is that cloud is a work in progress. A quarter (25%) characterized themselves as still learning. Most (75%) are past the beginning stage. However, of those only 16% describe their cloud adoption as mature. For most (59%), cloud adoption is still in process.



The new world of IT is not just about changing technology, it is also about the processes and organization of the people that turn core technologies into business solutions. One of the key changes to process happening among IT teams is the adoption of DevOps, a cultural-centric approach to combining development with operations — hence DevOps — to more effectively deliver applications. More than three quarters (76%) of those who have made an investment in cloud have adopted DevOps.

However, as we saw with cloud, DevOps adoption is evolving. Only a few (11%) characterize their adoption of DevOps as mature. Most (65%), characterize their DevOps adoption as still in process.



Detailed Findings: Security in the cloud creates new challenges and need for collaboration

Cloud investment has a dramatic impact on security

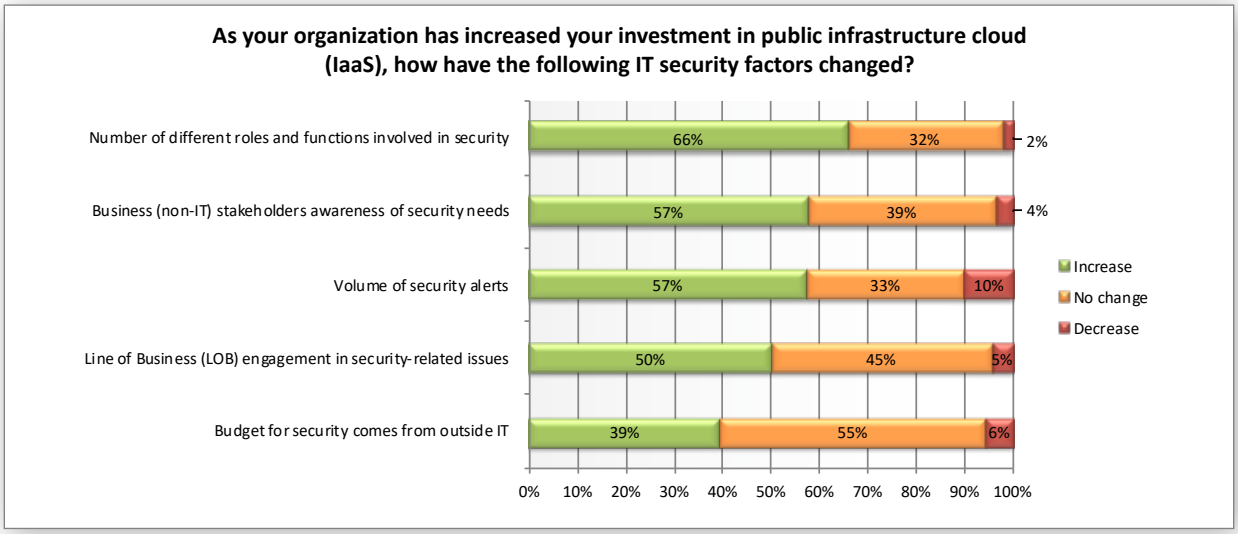
Moving from on-prem infrastructure to the cloud means change for the stakeholders responsible for security. We wanted to understand the change in five areas that impact security complexity including:

- Number of different roles and functions involved in security
- Business (non-IT) stakeholder awareness of security needs
- Volume of security alerts
- Line of business (LOB) engagement in security-related issues
- Budget for security coming from outside of IT

Along four of these five different security factors investigated, at least half have seen an increase. The security factor that changes most dramatically with the adoption of cloud is the number of different roles and functions that get involved in security-related activities with two-thirds (66%) reporting an increase in this area. For both awareness of security among non-IT stakeholders and volume of security alerts, well over half (57%) reported an increase. Half (50%) saw an increased in LOB engagement in security issues. Budget for security coming from outside IT saw the smallest increase, but that change was still reported by more than a third of companies (39%).

Each of these factors represents an increase in the complexity of security in cloud environments. Taken together, there is a clear picture of a security landscape that is much more complicated than traditionally found on-prem.

It should be noted that a handful of security stakeholders reported a decrease across all five security factors, but these were typically the minority, ranging from 2% to 10%.



Cloud security creates new organizational challenges

As we consider changing security factors in the above section, we see that many of these changes are organizational – more roles and functions are involved, including LOB teams that haven't traditionally needed to be heavily involved in security. These changes have created many challenges that directly relate to organization and the skills of the teams involved with security. The vast majority of security stakeholders (97%) report that they face organizational challenges in their cloud environments.

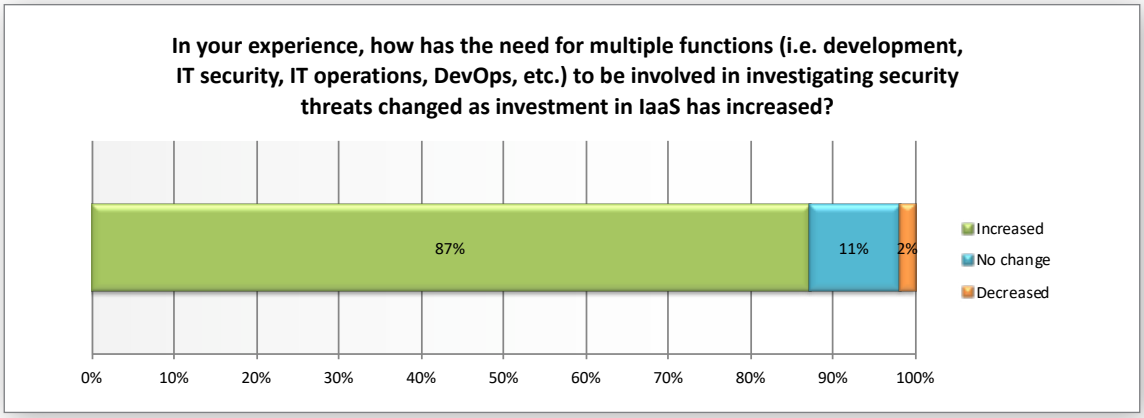
The most frequently reported issue (63%) is that cloud security requires broader technical expertise to understand threats. This issue is fundamental to securing an environment since if teams don't understand a threat, they have no way to address it.

Organizational challenges reported also included a need for greater cross-team coordination (54%), staff being overloaded (51%), cloud threats requiring greater business understanding to evaluate context (44%), and difficulty hiring cloud security expertise (33%). Several participants also took the time to write in "Other" organizational challenges they face. These included issues related to an increased split in authority between IT and security teams, lack of funding, requiring more input from their vendors, and that security problems in the cloud are "just harder."

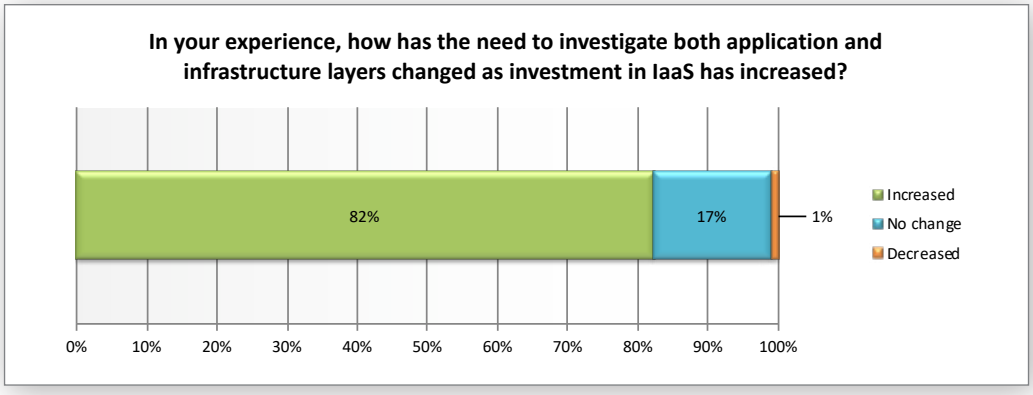
Security in the cloud requires an increase in collaboration

To drill further into these organizational challenges, we asked specific questions about the changes that security stakeholders have experienced as they investigate security threats. It is clear that security complexity increases in the cloud, for both organization and technology factors.

When asked specifically about the need to involve multiple functions or organizations to investigate a security threat for the cloud, we see that the majority of security stakeholders (87%) report this has increased. In cloud environments, it is much more likely that some mix of development, security, operations, DevOps, or other teams will be needed for security than has been required in the past.

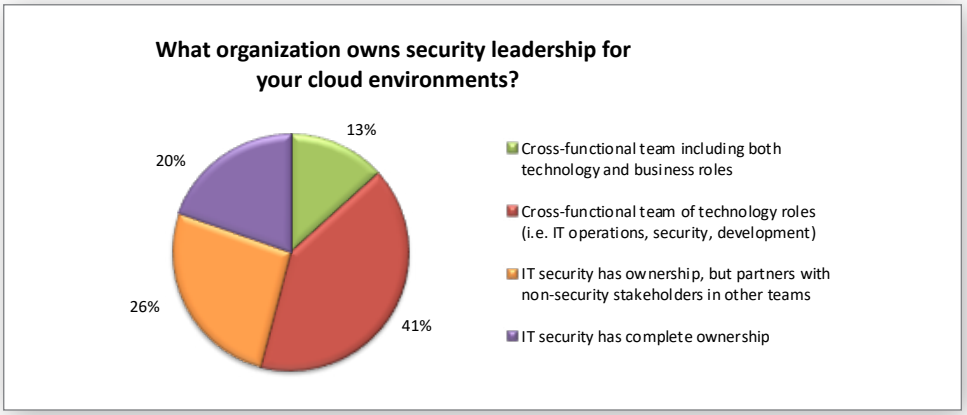


In a related question, we asked about technology layers. In cloud environments, more than 4 in 5 (82%) report that the need to consider both application and infrastructure layers when investigating a security threat increases.



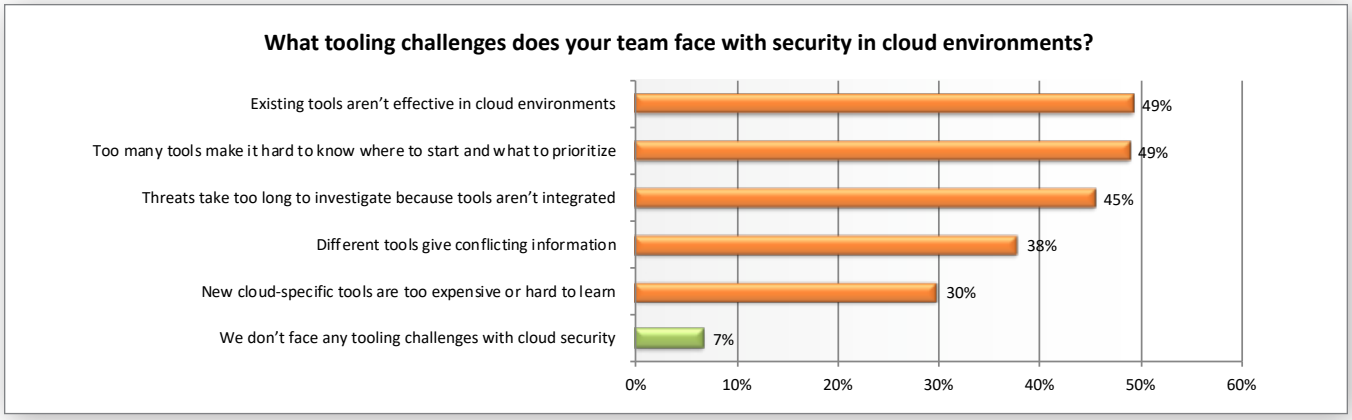
Security in the cloud is typically headed by cross-functional teams

IT teams are already adjusting security ownership to the new reality of the cloud. Only 1 in 5 (20%) continue to operate in the traditional manner, with the security department owning security leadership as a standalone group. More than half (52%) report that a cross-functional team has security leadership for cloud, although only a minority of these (13%) include business roles on those teams. For about a quarter (26%) security continues to take point, but with clear partners in non-security roles.



Most have challenges with existing tools for cloud security

Organizational issues are not the only challenges that arise with the adoption of cloud. Most cloud security stakeholders (93%) also report challenges with their security toolset. Half (49%) report the very alarming claim that existing tools simply aren't effective for cloud environments. Another half (49%) report that they have too many tools which creates challenges in knowing where to start. Integration is another issue for almost half (45%) because lack of integration means threats take too long to investigate. More than a third (38%) face challenges with different tools giving conflicting information.

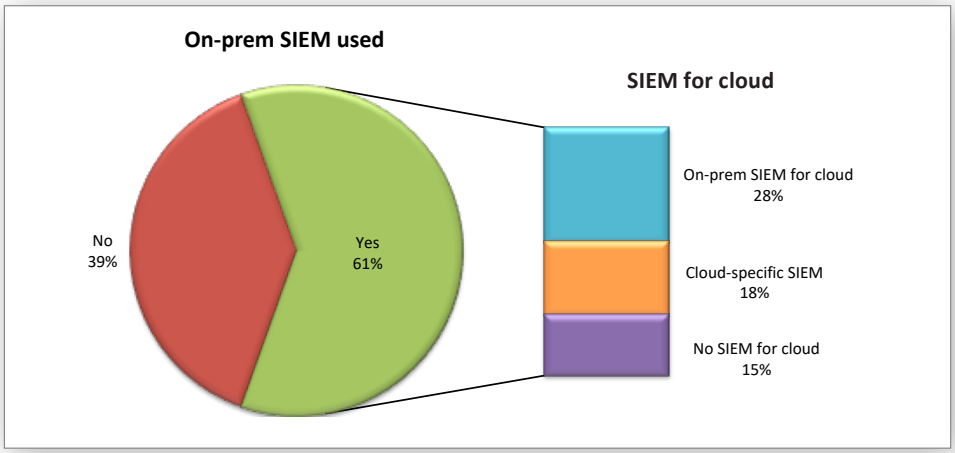


Detailed Findings: Traditional on-prem SIEM solutions are not a fit for cloud

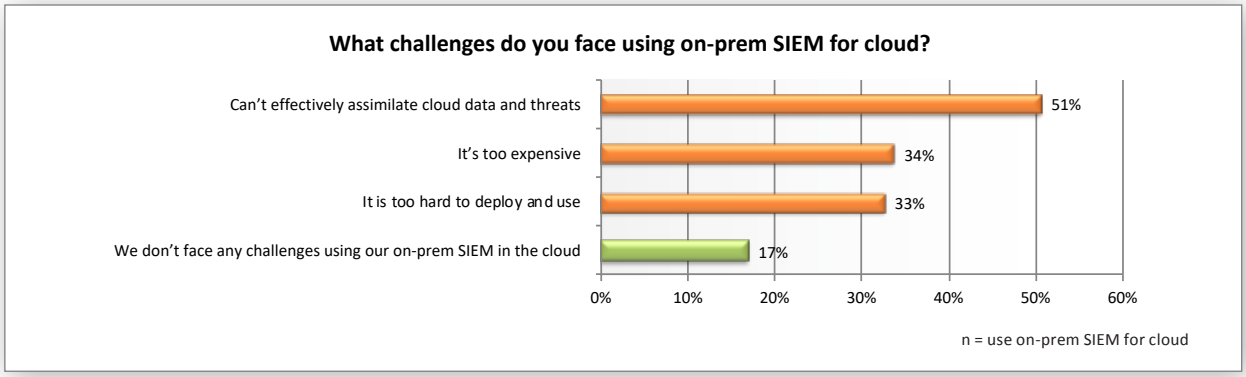
Organizations that use on-prem SIEM solutions in the cloud struggle

Security Information and Event Management (SIEM) tools have traditionally been used as a way to centralize and examine security alerts coming from throughout the infrastructure. Among the stakeholders in our survey, about two-thirds (61%) report the use of SIEM solutions in their on-prem environments.

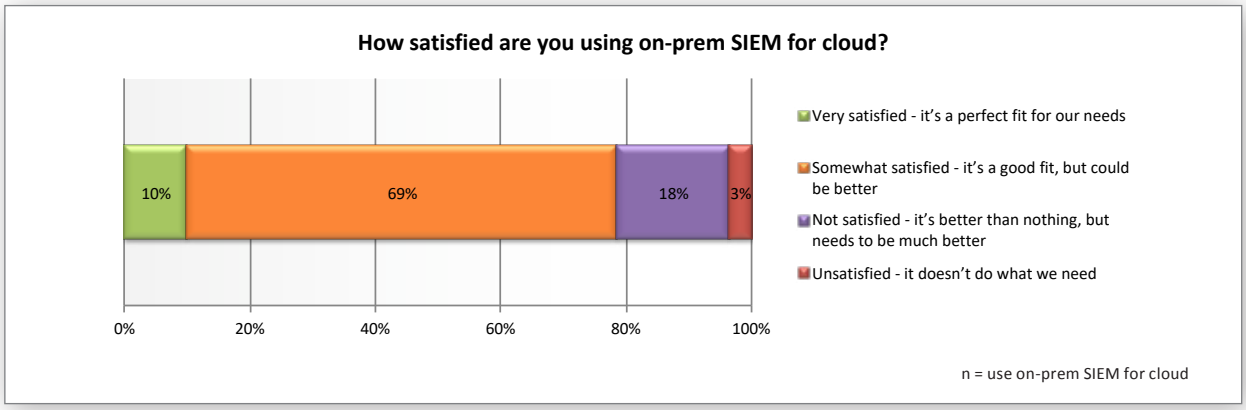
Among existing SIEM users, there is little consistency in how that translates to their cloud environment. Less than half of those use their on-prem SIEM for cloud, with the rest split between having invested in a cloud-specific SIEM and those who haven't adopted any kind of SIEM in the cloud.



Although there is no consistent approach to using SIEM in the cloud, what is consistent is that the people who try to use their on-prem SIEM for cloud environments are struggling. Most of them (83%) face challenges, with half (51%) reporting that the issue is that their on-prem SIEM can't effectively assimilate cloud data and threats. This is particularly concerning as the main purpose of SIEM is to do just that!



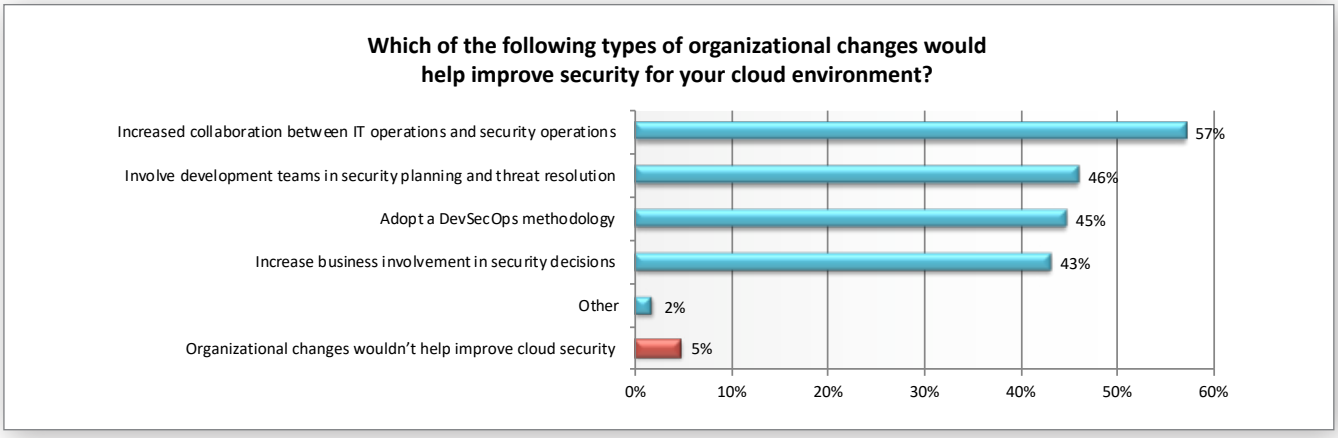
Given these challenges, it is not surprising that there is a lack of satisfaction among teams that use their on-prem SIEM for their cloud environments. Only 10% report that they are fully satisfied with that approach.



Detailed Findings: New models are needed to break down silos of people, workflow, and technology

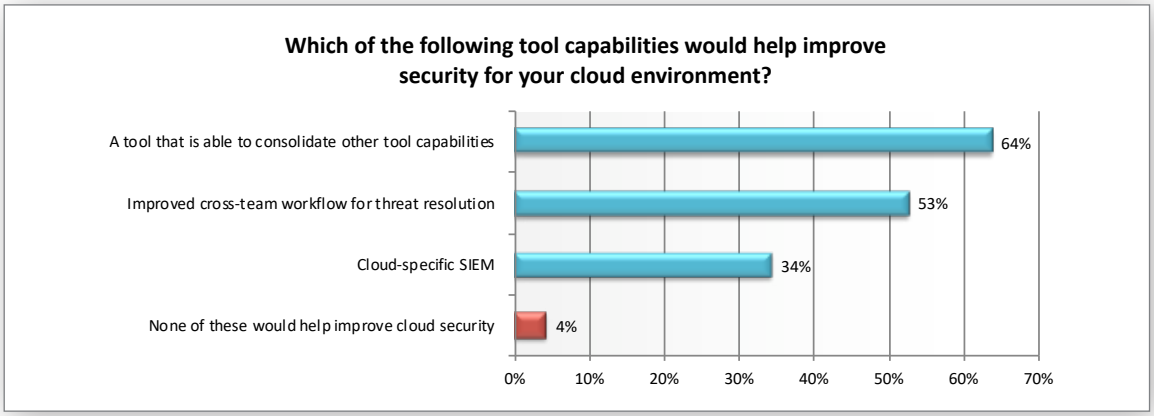
Cloud security would benefit from organizational changes

As we saw above, the move to cloud creates many organizational challenges, so it is not surprising that most (95%) security stakeholders report that cloud security would be improved if changes were made to the way their teams work including increasing collaboration between the IT operations and security operations teams (57%), involving development teams in security planning and threat resolution (46%), adopting a DevSecOps methodology to introduce security earlier in the application lifecycle (45%), and increasing business involvement in security decisions (43%). Some participants reported "Other" organizational changes that would help including increasing budget and investment, as well as offering increased training for both technology stakeholders and end-users.



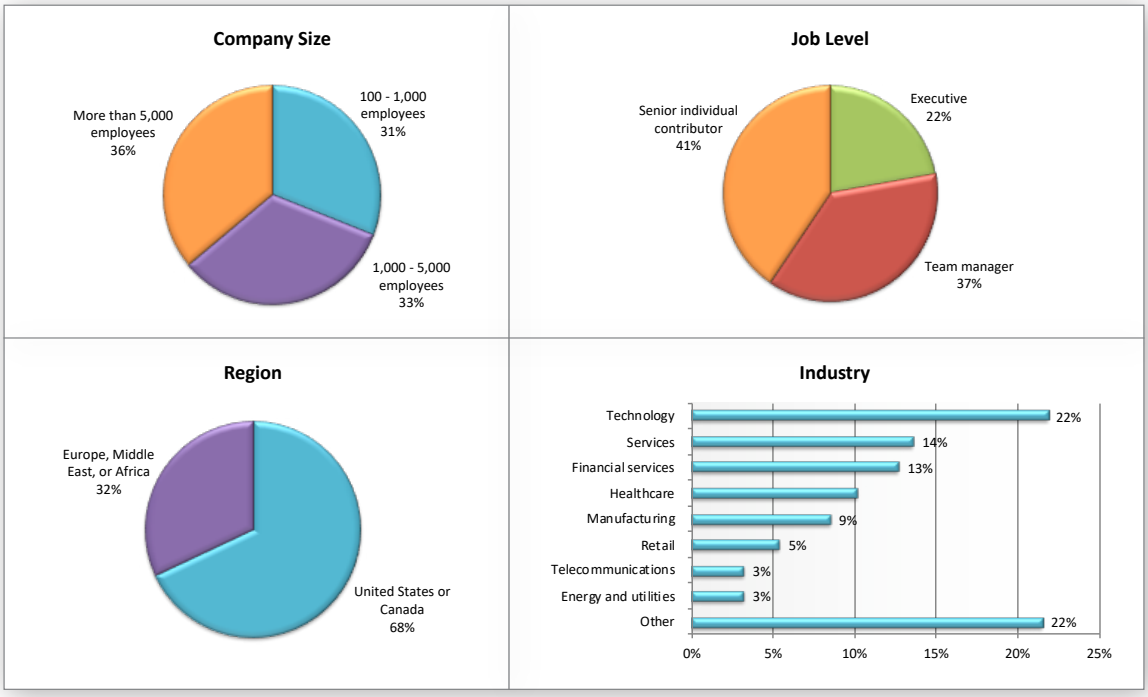
New security capabilities desired for cloud environments

Along with organizational changes, most security stakeholders (96%) report their teams would deliver better security outcomes from tool changes including consolidation of existing tool capabilities (64%), improved cross-team workflows for threat resolution (53%) and cloud-specific SIEM (34%).



Survey Methodology and Participant Demographics

An online survey was sent to independent sources of IT security professionals. A total of 316 qualified decision makers completed the survey. All participants were responsible for security in environments with significant investments in both cloud (public IaaS) and on-prem infrastructure. Participants included a mix of job levels, company sizes, and industries.



About Dimensional Research

Dimensional Research® provides practical market research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT. We understand how technology organizations operate to meet the needs of their business stakeholders. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information, visit dimensionalresearch.com.

About Sumo Logic

Sumo Logic is a secure, cloud-native, machine data analytics service, delivering real-time, continuous intelligence from structured, semi-structured and unstructured data across the entire application lifecycle and stack. More than 1,600 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a multi-tenant, service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, CA and is backed by Accel Partners, DFJ, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital and Sutter Hill Ventures. For more information, visit www.sumologic.com.