ESG a division of TechTarget

Enterprise Strategy Group | Getting to the bigger truth.™

Beyond Cloud Adoption:
How to Embrace the Cloud for Security and Business Benefits

PREPARED BY ESG FOR:

DEVO

TABLE OF CONTENTS

Research Objectives

As organizations embrace public cloud apps and infrastructure, they must rethink the tools, processes, and people employed to secure their expanded attack surface. This survey was designed to measure the pace of change in the market, both in terms of cloud adoption and evolving security practices. The crux of the research is focused on understanding the correlation between organizations' approaches to cloud security and their cloud security successes and failures: **do organizations taking different approaches to cloud security experience materially different security outcomes?**

To explore the answers to these and other questions, ESG surveyed 500 IT and security personnel in the 'SOC chain of command' at their organizations.

THIS STUDY SOUGHT TO:

Assess the usage of public cloud computing and the pace of change at organizations.

Determine whether and how cloud computing is changing security practices and technologies.

Understand how organizations with different approaches to securing the cloud experience different cloud outcomes.

Back to Contents

Research Highlights

Leading organizations are aggressively adopting cloud computing and moving security technologies to the cloud.

ESG calls these organizations “Cloud Evangelists.” To address cloud computing security challenges, Cloud Evangelists are taking decisive actions such as increasing security training and budgets, adopting cloud-based security data lakes, and even adding a second SIEM dedicated to security monitoring for cloud-based applications and workloads.

Data volume and increased threats are driving the move of security technologies to the cloud.

To address scaling needs while streamlining operations, many organizations are moving security technologies to the cloud. The goal? Comprehensive visibility in an increasingly complex hybrid IT infrastructure.

Cloud computing drives security complexity.

As cloud computing applications and workloads proliferate, organizations experience a rapid increase in IT and security complexity. From a security perspective, cloud computing adoption requires new security skills, increases volume of security telemetry, and opens organizations to new types of security threats.

The cloud computing train has left the station.

Organizations large and small are moving workloads to the cloud, developing cloud-native applications, and embracing SaaS applications. These trends have accelerated to address requirements driven by the global pandemic.

Back to Contents

Cloud computing adoption is on the rise

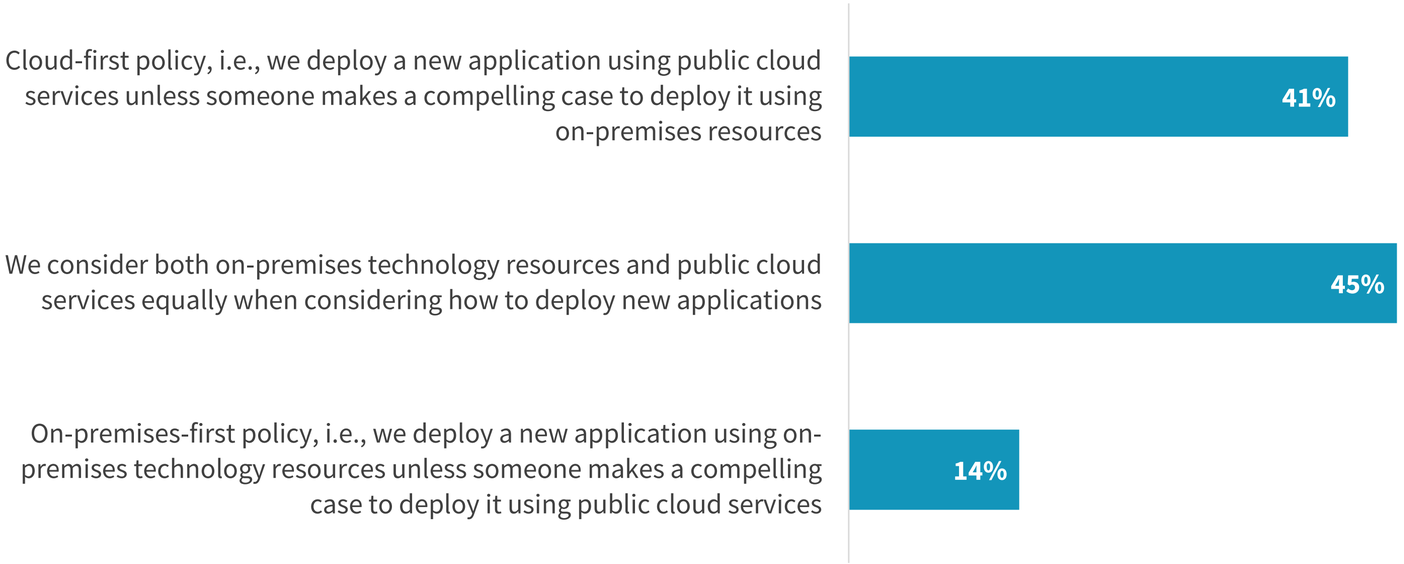
According to ESG research, most organizations are well past the tipping point for cloud computing proliferation. For example:

- **More than one-third (34%) of organizations claim that at least half of their applications and workloads reside in public cloud infrastructure today.** This will increase precipitously in the near future. 53% of organizations believe that at least half of their applications and workloads will reside in the public cloud two years from now.
- **41% of organizations have adopted a cloud-first policy, deploying new applications using public cloud services by default.** Alternatively, only 14% of organizations maintain a policy where new applications are deployed using on-premises technology.
- **90% of organizations claim that they have increased their use of public cloud computing as a result of the global pandemic.** Furthermore, 81% of organizations accelerated plans and timelines for public cloud computing in response to new requirements driven by the global pandemic.

> *"**90% of organizations** claim that they have increased their use of public cloud computing as a result of the global pandemic."*

Clearly, organizations are past the "early adopter" phase of cloud computing where security concerns prevented rapid cloud propagation. As organizations embrace the public cloud and accelerate utilization, CISOs must adjust their security strategies to prevent, detect, and respond to cyberattacks on cloud-based applications and data.

Organizations' use of the public cloud when deploying new applications.



Back to Contents

Security technologies are migrating to the cloud

The research shows that security technologies are following a similar pattern to cloud adoption. They are migrating from on-premises to cloud- and SaaS-based alternatives.

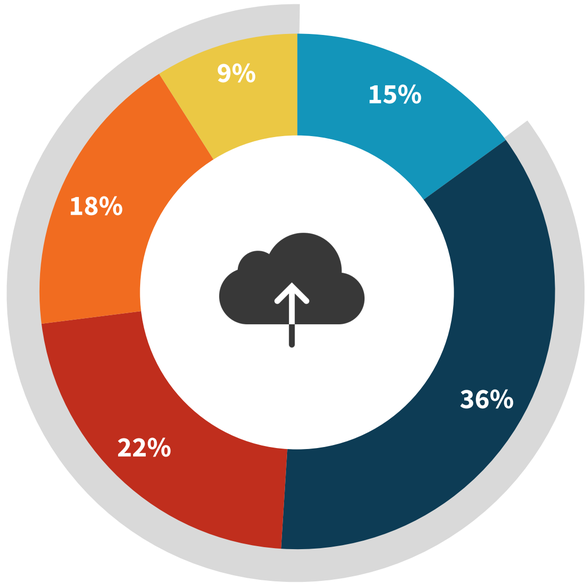
- **39% of organizations have adopted a cloud-first strategy as they select and deploy new security technologies.** Alternatively, 16% of organizations maintain a preference for on-premises security technology.
- 43% of organizations claim that at least half of their security tools and controls are now deployed in the cloud. **In 2 years, 56% of organizations believe that at least half of their security tools and controls will be deployed in the cloud.**
- Organizations are particularly active in moving security information and event management (SIEM) systems to the cloud: **The majority (85%) of organizations either rely on a SIEM SaaS provider, have "lifted and shifted" on-premises SIEM to the cloud, or are in the process of adopting a cloud SIEM strategy** (i.e., by moving on-premises SIEM to the cloud or switching to a SaaS-delivered SIEM solution).

> ***91%*** *say that they've achieved greater SIEM scalability"*

Respondents who use a SaaS SIEM have noted numerous benefits. 91% say that they've achieved greater SIEM scalability, 87% report greater visibility, and 85% see greater uptime/availability.

While only 9% of the survey population currently uses a SaaS SIEM, another 22% plan on switching from an on-premises SIEM to a SaaS-delivered solution.

SIEM deployment preferences.



Back to Contents

The Rise of the Cloud Evangelist

Three approaches to cloud adoption and security

The research indicates that organizations are increasing their use of cloud computing AND moving security technologies to the cloud as a rule.
To understand the ramifications of these changes, ESG created a segmentation model that divided participating organizations into 4 categories based upon their adoption of cloud computing for business applications and workloads as well as their adoption of cloud-based security controls. The four segments are:

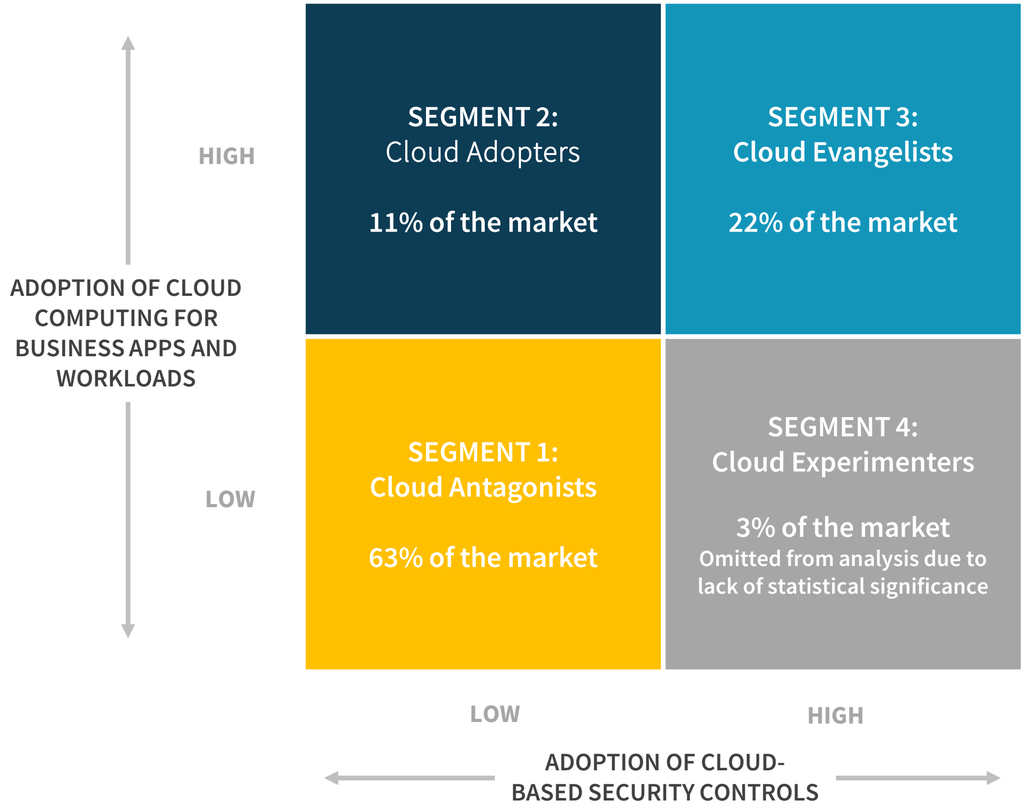
1. Cloud Antagonists (63% of the survey population) are those organizations that are not aggressively adopting either cloud computing for business apps/workloads or cloud-based security controls.

2. Cloud Adopters (11% of the survey population) are those organizations that are adopting cloud computing for business apps/workloads but are not as aggressive toward adoption of cloud-based security controls.

3. Cloud Evangelists (22% of the survey population) are those organizations with both high adoption of cloud computing for business apps/workloads and high adoption of cloud-based security controls.

4. Cloud Experimenters are those organizations that are adopting cloud-based security controls but are not as aggressive toward adoption of cloud computing for business apps/workloads. As this type of organization is very rare, data from this segment has been omitted from this eBook due to a lack of statistical representation.

As it turns out, an organization's cloud computing and security strategy can yield vastly different IT and business results.



Respondents were placed into one of three segments based on their responses to 2 questions:

1. To the best of your knowledge, approximately what percentage of your company's applications and workloads reside in any public cloud (e.g., in a SaaS service or on a PaaS/IaaS platform)?

High: >50% Low: 50% or less

2. Thinking specifically of cybersecurity tools and controls in use at your organization, approximately what percentage reside in any public cloud (e.g., in a SaaS service or on a PaaS/IaaS platform) today?

High: >60% Low: 60% or less

Back to Contents

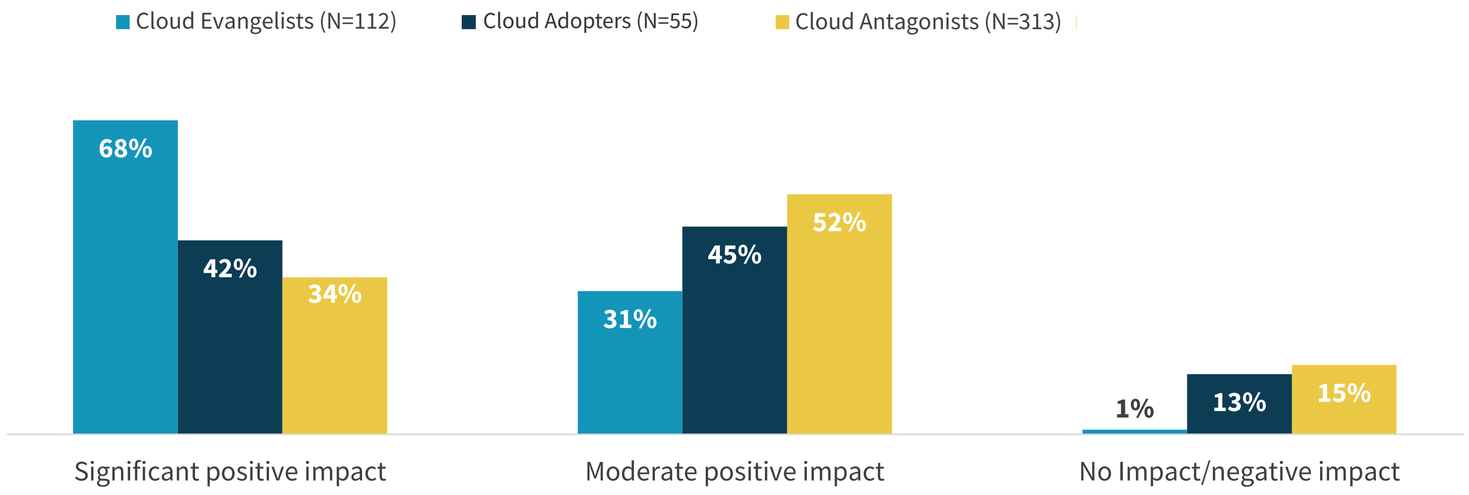
Cloud security investment directly impacts business benefits

Aggressive adoption of cloud computing for business applications, workloads, and security technologies delivers a strong return on investment. As an example, 68% of Cloud Evangelists claim that public cloud computing has had a significantly positive impact on the business, compared to Cloud Adopters (42%) and Cloud Antagonists (34%). Far from an anomaly, Cloud Evangelists had several other more encouraging results. For example:

- **53% of Cloud Evangelists** report that cloud computing has had a significantly positive impact on the pace of application development/deployment as compared to Cloud Adopters (38%), and Cloud Antagonists (29%).
- **62% of Cloud Evangelists** report that cloud computing has had a significantly positive impact on the pace of adopting new technologies as compared to Cloud Adopters (42%) and Cloud Antagonists (31%).

> *68% of Cloud Evangelists claim that* ***public cloud computing has had a significantly positive impact on the business.***

The impact public cloud utilization has had on the business.



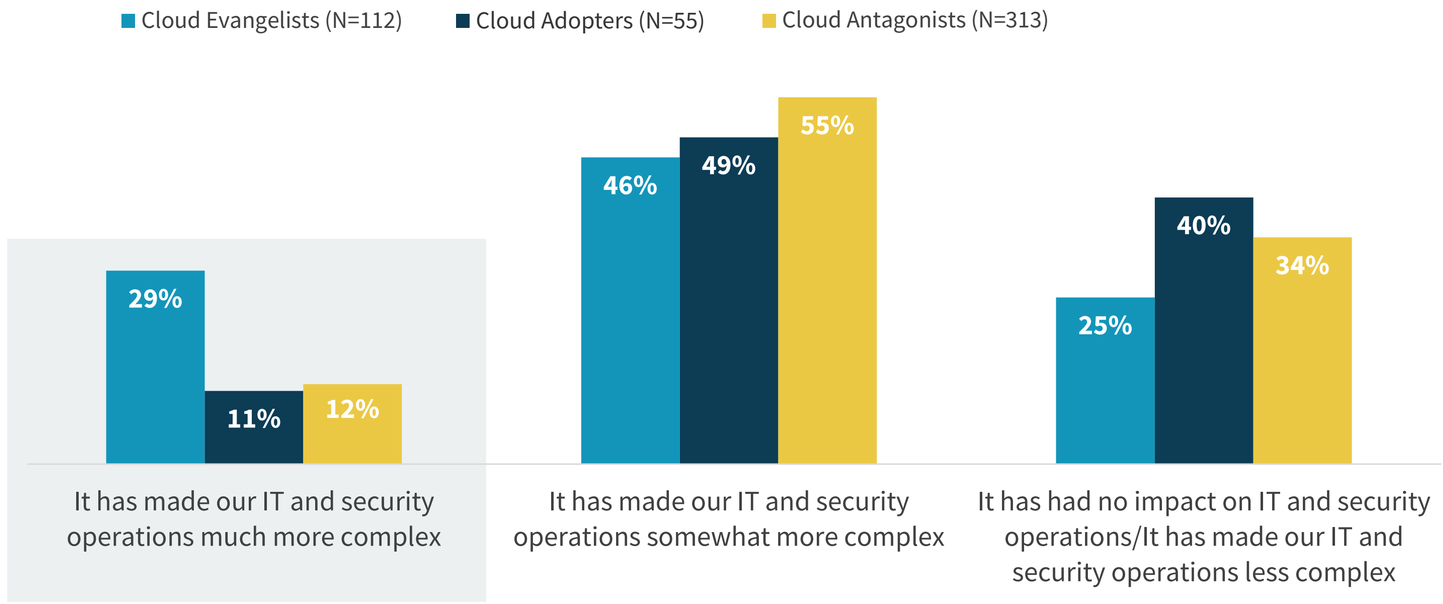
Back to Contents

Security complexity comes with cloud evangelism

While Cloud Evangelists reap strong business and IT benefits, these advantages aren't free. For example, the research indicates that 29% of Cloud Evangelists believe that public cloud computing has made their IT and security operations much more complex—more than 2 times higher than Cloud Adopters (11%) or Cloud Antagonists (12%). Additionally:

- **30% of Cloud Evangelists** strongly agree that their adoption of cloud computing exposes them to new and more complex cyberattacks, compared to 16% of Cloud Adopters and 19% of Cloud Antagonists.
- **30% of Cloud Evangelists** strongly agree that their adoption of cloud computing has exposed limitations in their organization's ability to provide complete security visibility, compared to 24% of Cloud Adopters and 18% of Cloud Antagonists.
- **29% of Cloud Evangelists** strongly agree that their adoption of cloud computing has exposed limitations in their existing security toolsets, compared to 18% of Cloud Adopters and 19% of Cloud Antagonists.
- **38% of Cloud Evangelists** strongly agree that their adoption of cloud computing has led to an increase in security data for analysis, compared to 27% of Cloud Adopters and 29% of Cloud Antagonists.
- **30% of Cloud Evangelists** strongly agree that their adoption of cloud computing has caused them to evaluate new/specialized cloud security technologies, compared to 24% of Cloud Adopters and 18% of Cloud Antagonists.

The impact public cloud utilization has had on security operations.



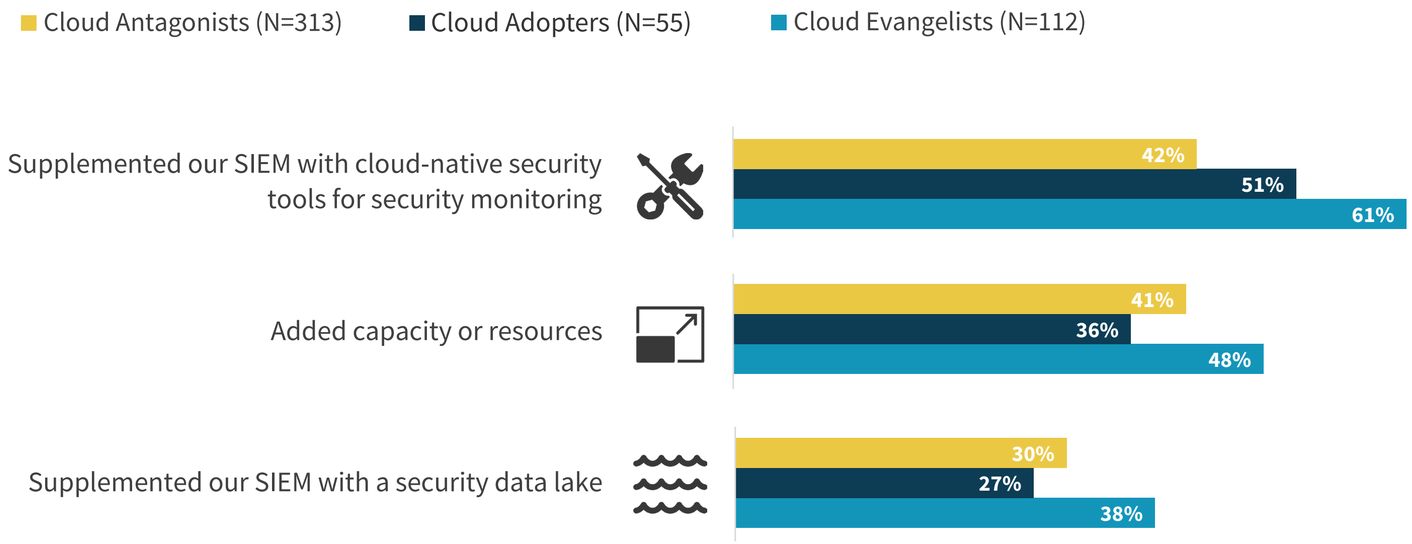
Back to Contents

Cloud Evangelists take more decisive security actions

Cloud evangelism clearly comes with numerous security challenges. To address them, Cloud Evangelists are taking additional security actions. For example:

- **61% of Cloud Evangelists** are supplementing SIEM with cloud-native security monitoring tools, compared to 51% of Cloud Adopters and 42% of Cloud Antagonists. This gives Cloud Evangelists more detailed visibility into cloud security posture and behavior.
- **48% of Cloud Evangelists** are adding capacity or resources, compared with 36% of Cloud Adopters and 41% of Cloud Antagonists. This action is meant to address the additional workload and security complexity of cloud computing.
- **38% of Cloud Evangelists** are supplementing their SIEM with a security data lake, compared with 27% of Cloud Adopters and 30% of Cloud Antagonists. This helps organizations address growing data volumes for activities like threat hunting and forensic investigations.
- **38% of Cloud Evangelists** are adding a second SIEM dedicated to monitoring/managing cloud security, compared with 25% of Cloud Adopters and 25% of Cloud Antagonists. Evangelists are adopting additional SIEMs that run in the cloud with the scale, capacity, and design points to keep up with cloud innovation. Often, Evangelists run multiple SIEMs and eventually migrate all security visibility use cases to a cloud-based SIEM.

Actions taken to accommodate public cloud utilization.



Back to Contents

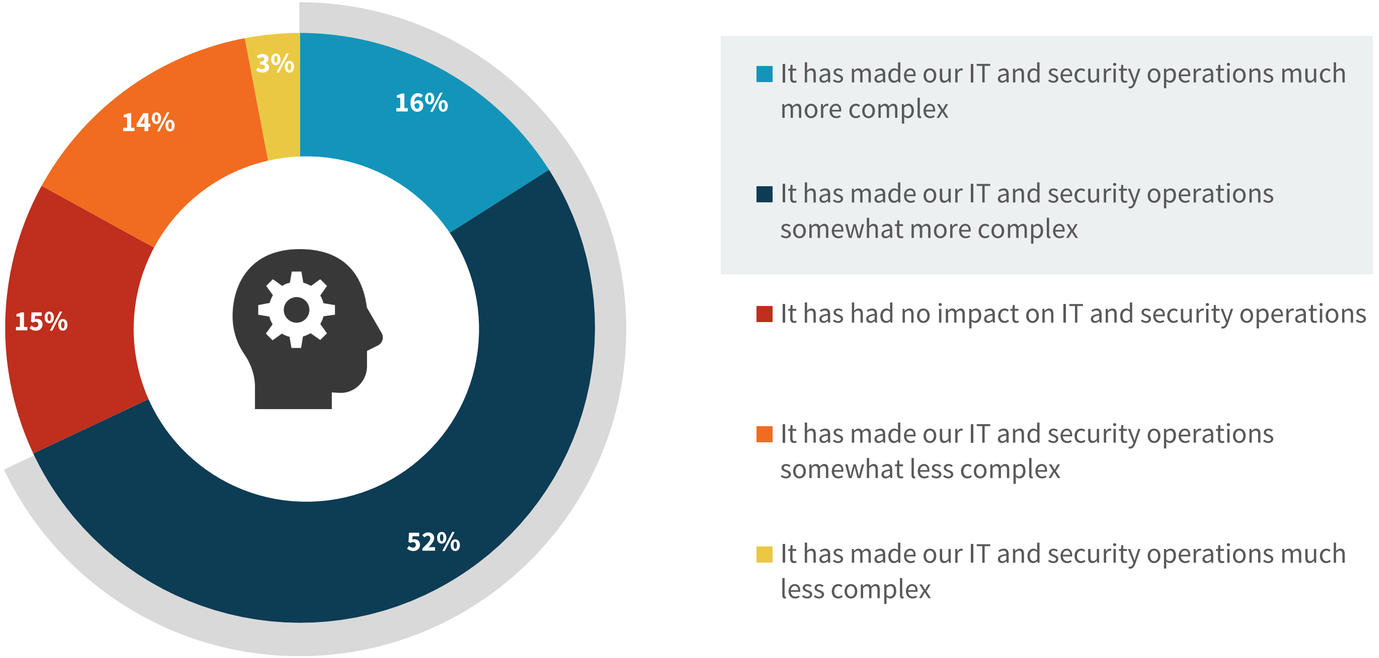
Cloud computing drives security complexity

As all organizations accelerate cloud computing initiatives, they must be prepared for an unwelcome byproduct: operational complexity. The research illustrates that 68% of organizations believe that cloud computing has made IT and security operations much more or somewhat more complex. The research also indicates an adverse relationship—the more aggressively organizations pursue cloud computing, the more complex IT and security operations become.

What's driving this complexity? 41% say that cloud computing has increased the IT and security workload, 35% claim that the use of public cloud computing requires new skills, 28% point to a lack of familiarity with the cloud security shared responsibility model, and 25% report problems moving existing security policies and controls with public cloud computing.

> *68% believe that cloud computing has made* ***IT and security operations more complex.***

The impact public cloud utilization has had on security operations.



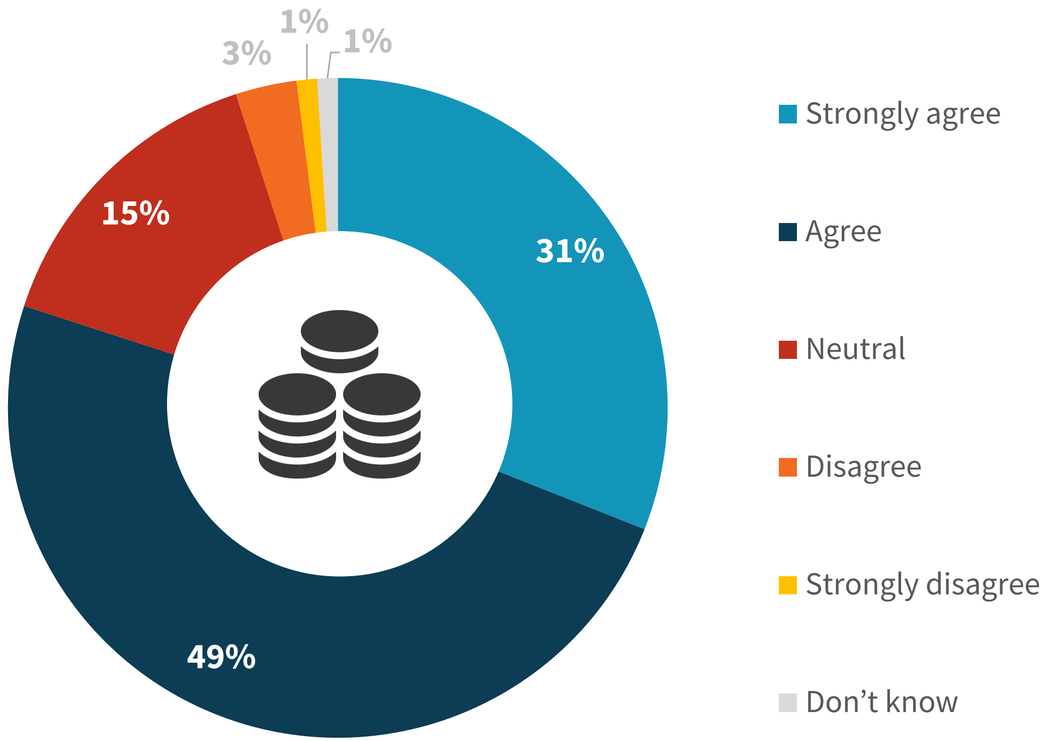
Back to Contents

> ***80% of survey respondents agree*** *that cloud computing has led to an increase in the amount of security data to analyze.*”

Cloud computing is increasing security telemetry volume

In addition to more complexity, the vast majority of organizations are dealing with an increase in security telemetry—80% of survey respondents agree that cloud computing has led to an increase in the amount of security data to analyze. This increase can easily overwhelm the SOC team or lead to performance and scalability issues with existing logging and analytics tools.

Agree or disagree: my organization’s use of cloud computing has led to an increase in security data to analyze.



Back to Contents

Organizations have limited confidence in security visibility of cloud-resident workloads

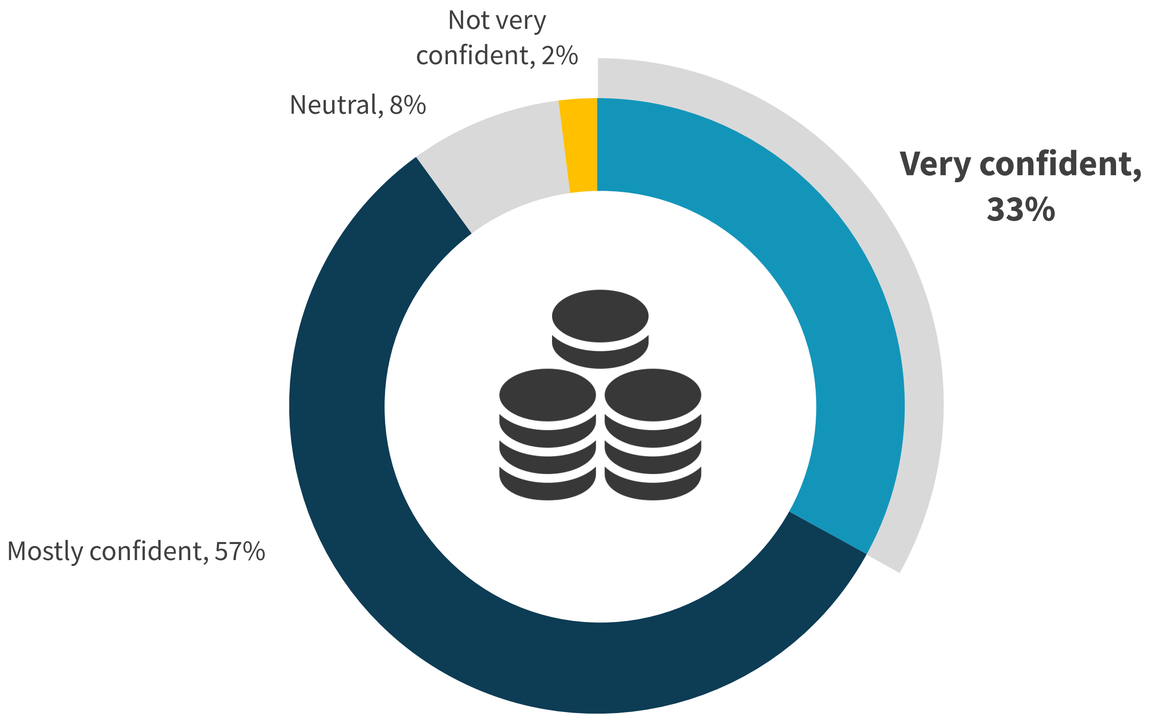
With increases in both complexity and data volume, the cloud computing explosion has also led to visibility gaps that impact the SOC team's ability to measure cyber risk, monitor behavior, and respond to events.

As the old management adage states, "You can't manage what you can't measure." Extrapolating this to a cloud security context, organizations can't implement the right controls, detect suspicious activities, or respond to events without the right level of visibility and oversight.

Given the rapid adoption of IaaS, PaaS, and SaaS, visibility gaps could lead to devastating and costly cyberattacks. As the research indicates, many firms are moving SIEM to the cloud, as a SaaS SIEM can increase processing/storage capacity for greater data ingestion, advanced analytics, and end-to-end visibility.

> *"**Only one-third of organizations** claim they are very confident that their organization's tools provide adequate security visibility into cloud-resident workloads."*

Confidence that the security team has adequate visibility into the cloud.



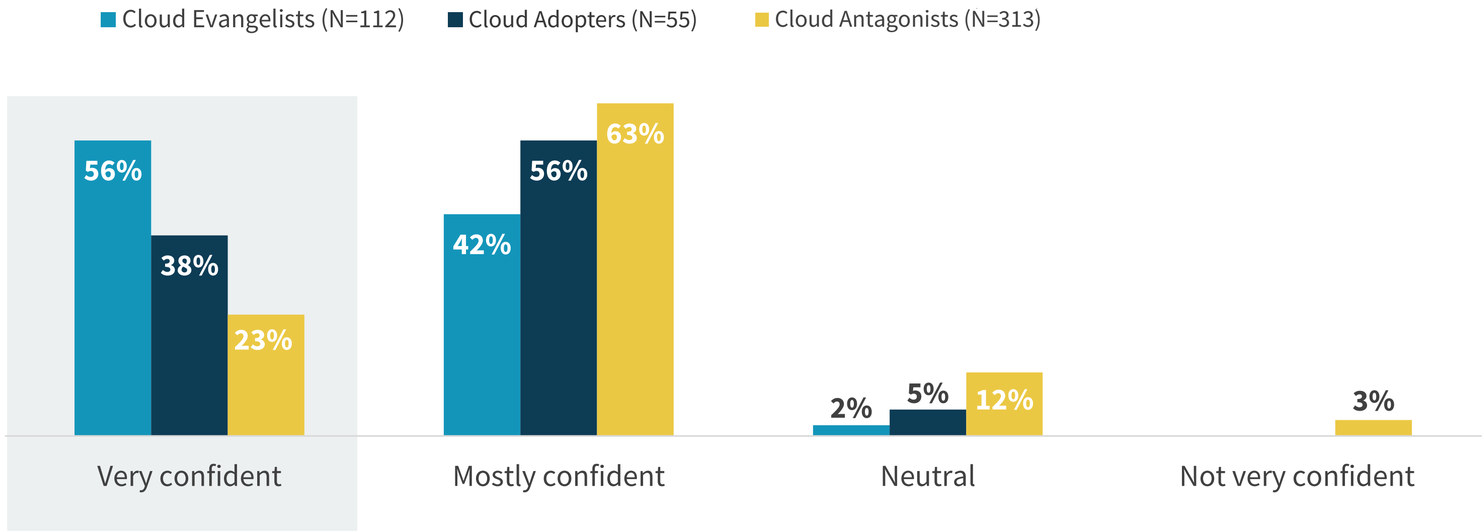
Back to Contents

Cloud Evangelists are more confident in security visibility

Though Cloud Evangelists say that cloud computing increases the complexity of their IT and security operations, they are getting the benefit of higher visibility.

By adding resources, adopting cloud-based security controls, implementing a security data lake, and deploying a second SIEM, Cloud Evangelists gain more comprehensive security visibility. Indeed, 56% of Cloud Evangelists are very confident that their organization's tools provide adequate security visibility into cloud-resident workloads, compared to 38% of Cloud Adopters and 23% of Cloud Antagonists.

Confidence that the security team has adequate visibility into the cloud.



> ***56% of Cloud Evangelists are very confident*** *that their organization's tools provide adequate security visibility into cloud-resident workloads"*

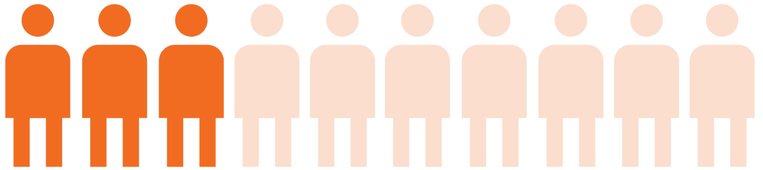
Back to Contents

Cloud computing is not immune to cyberattacks

Security complexity, growing security data volumes, and visibility gaps should cause alarm bells to ring in the CISO's office for one simple reason—nearly half (47%) of organizations have experienced at least one cyberattack specifically related to their public cloud environment over the past year.

Proportion of organizations that have suffered a cloud-specific cybersecurity attack.

81%
have experienced at least one cyberattack



28%
have experienced **several** attacks

Back to Contents

Organizations are altering security strategies to address cloud computing growth and security complexity

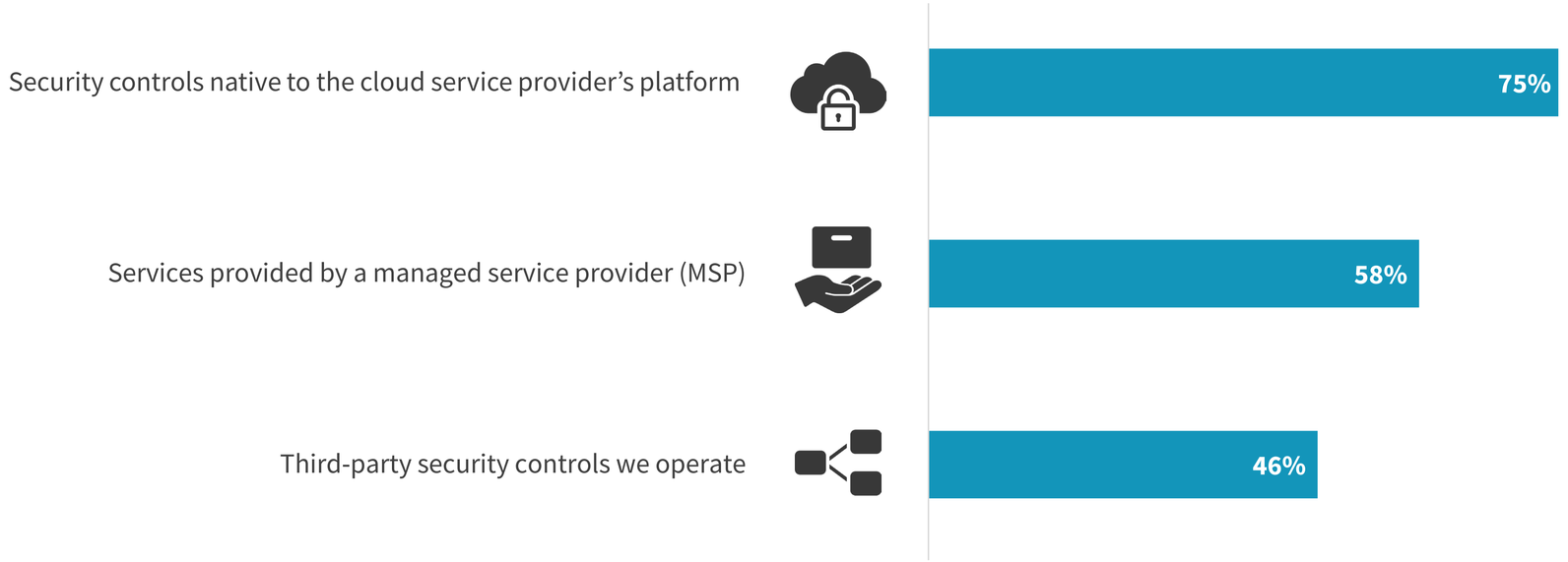
Infosec teams use a mix of security technologies for cloud-hosted applications

CISOs recognize these security challenges and are actively working to address operations complexity. As a first step, organizations are increasing cloud security spending. More than three-quarters (79%) of organizations expect cloud computing security spending to increase over the next 12 months.

Organizations are also using a diverse mix of security technologies for cloud security. Three-quarters (75%) use native cloud security controls, 58% turn to MSP services, and 46% operate third-party security controls. These efforts demand strong oversight, coordination, and persistent security staff training.

> **More than three-quarters (79%)** *of organizations expect cloud computing security spending to increase over the next 12 months.”*

Controls used to secure cloud-resident applications.



Back to Contents

Security operations teams take many different cloud security actions

Organizations are making significant changes to address security operations complexity. For example, 52% of organizations trained the SOC staff on cloud security, 47% supplemented their SIEM with cloud-native security tools for security monitoring, 43% automated security operations processes for cloud workload threat detection/response, 41% have added security capacity or resources, and 39% added SOC staff.

The data also indicates that legacy SIEM tools may be inadequate for addressing cloud-based security requirements. To bridge this gap, nearly one-third (31%) of organizations supplemented their SIEM with a security data lake while 29% actually added a second SIEM dedicated to monitoring/managing cloud security.

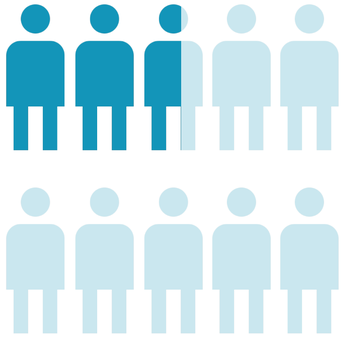
Actions taken to accommodate public cloud utilization.

Back to Contents

Many organizations seek specialized tools to protect cloud workloads

Organizations recognize the need to evolve their security practices and tool sets for cloud realities. When respondents were asked about their highest security priorities moving forward, a significant proportion (26%) reported a need to operate a dedicated SIEM system focused on the cloud environment. Another 25% reported the need to invest in tools with advanced analytics and which enable faster response to cloud threats.

Top priorities for security teams.



26%

Create a dedicated SIEM/log management system to monitor and manage public cloud security

25%

Create and/or purchase tools offering advanced security analytics to better detect and respond to threats targeting public cloud workloads

Back to Contents

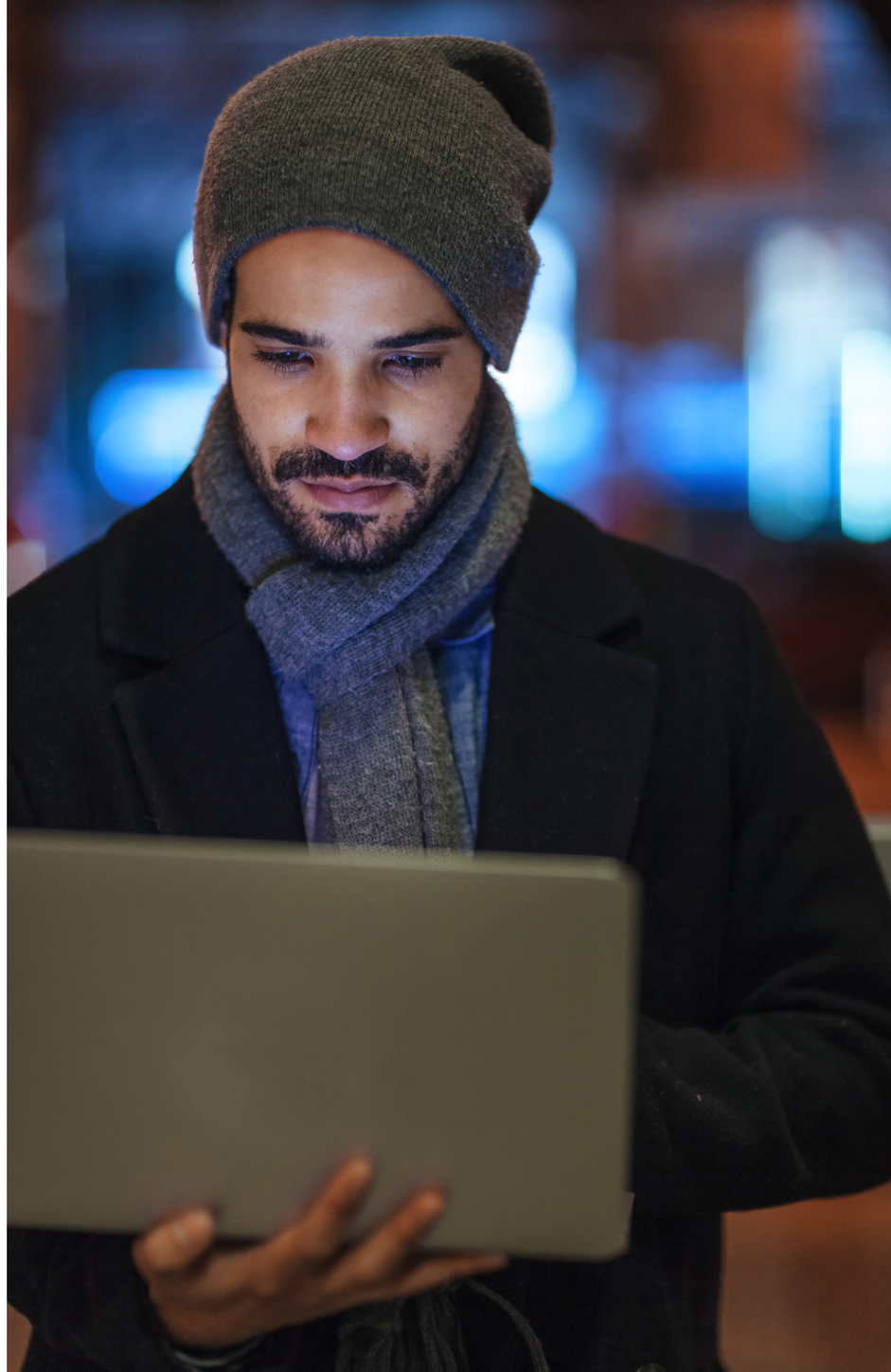
Recommendations for Security Professionals

Based upon the research presented in this eBook, organizations should be equipped for continuous and escalating use of cloud computing. While many organizations are following a similar course by migrating security technologies to the public cloud, this move alone is insufficient for dealing with cloud computing security complexity and scale.

To address these inevitable challenges, CISOs must:

- **Prepare their organization** by training the staff and increasing headcount to accommodate growing workloads. Security professionals must become cloud security experts.
- **Reinforce and test controls** for new types of cyberattacks targeting cloud-resident applications and data. This means collecting, processing, analyzing, and acting upon the right security data.
- **Get ready for massive growth** in security data volume by adopting cloud-native monitoring tools, moving security analytics to the cloud, and assessing whether current SIEM systems have the analytics capabilities, capacity, and performance to meet cloud-driven requirements. They should plan to supplement and/or replace legacy SIEM tools that can’t keep up.
- **Strive for full visibility** across hybrid IT infrastructure. This requires cloud-scale SIEM capabilities for data ingestion, high-performance query capabilities, and an intuitive user interface for security operations processes.

Back to Contents



Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow.

LEARN MORE

ABOUT ESG

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

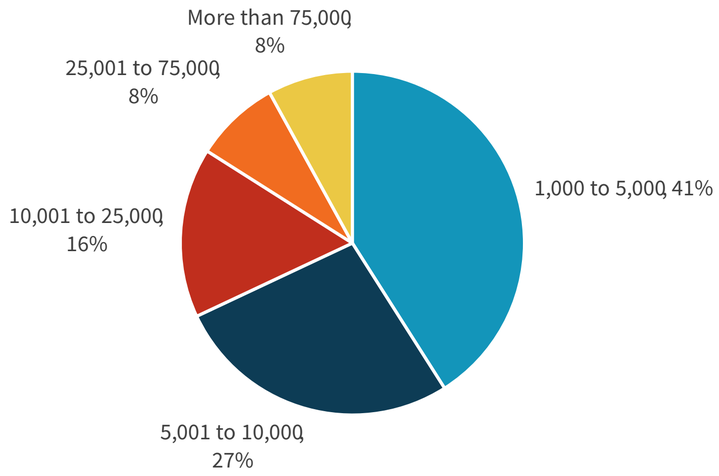
Research Methodology

To gather data for this eBook, ESG conducted a comprehensive online survey of IT and security personnel in the 'SOC chain of command' at their organization. Respondents were distributed across North America (50%) and Western Europe (50%), and all worked at organizations with 1,000 or more employees. The survey was fielded between January 11, 2021 and January 29, 2021.

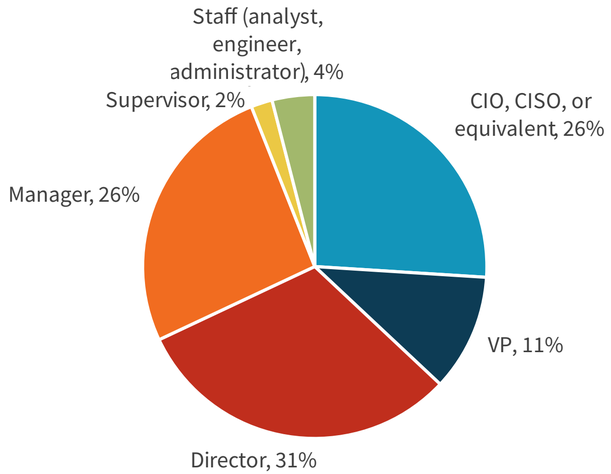
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 500 respondents remained.

All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding. The margin of error for a sample size of 500 is + or – 4 percentage points.

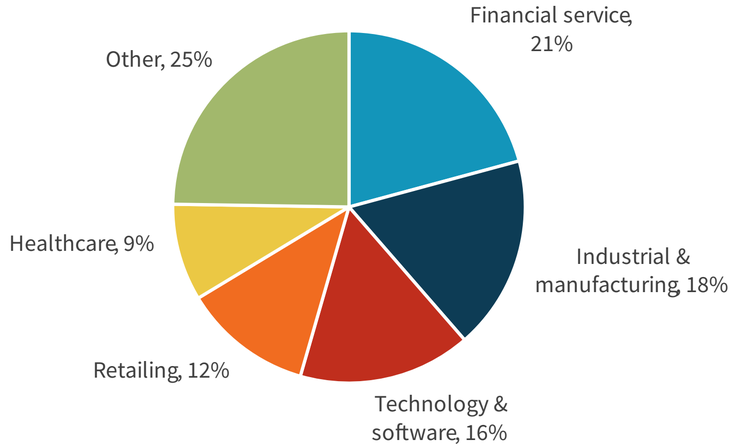
RESPONDENTS BY NUMBER OF EMPLOYEES (N=500)



RESPONDENTS BY ROLE (N=500)



RESPONDENTS BY INDUSTRY (N=500)



Back to Contents

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.