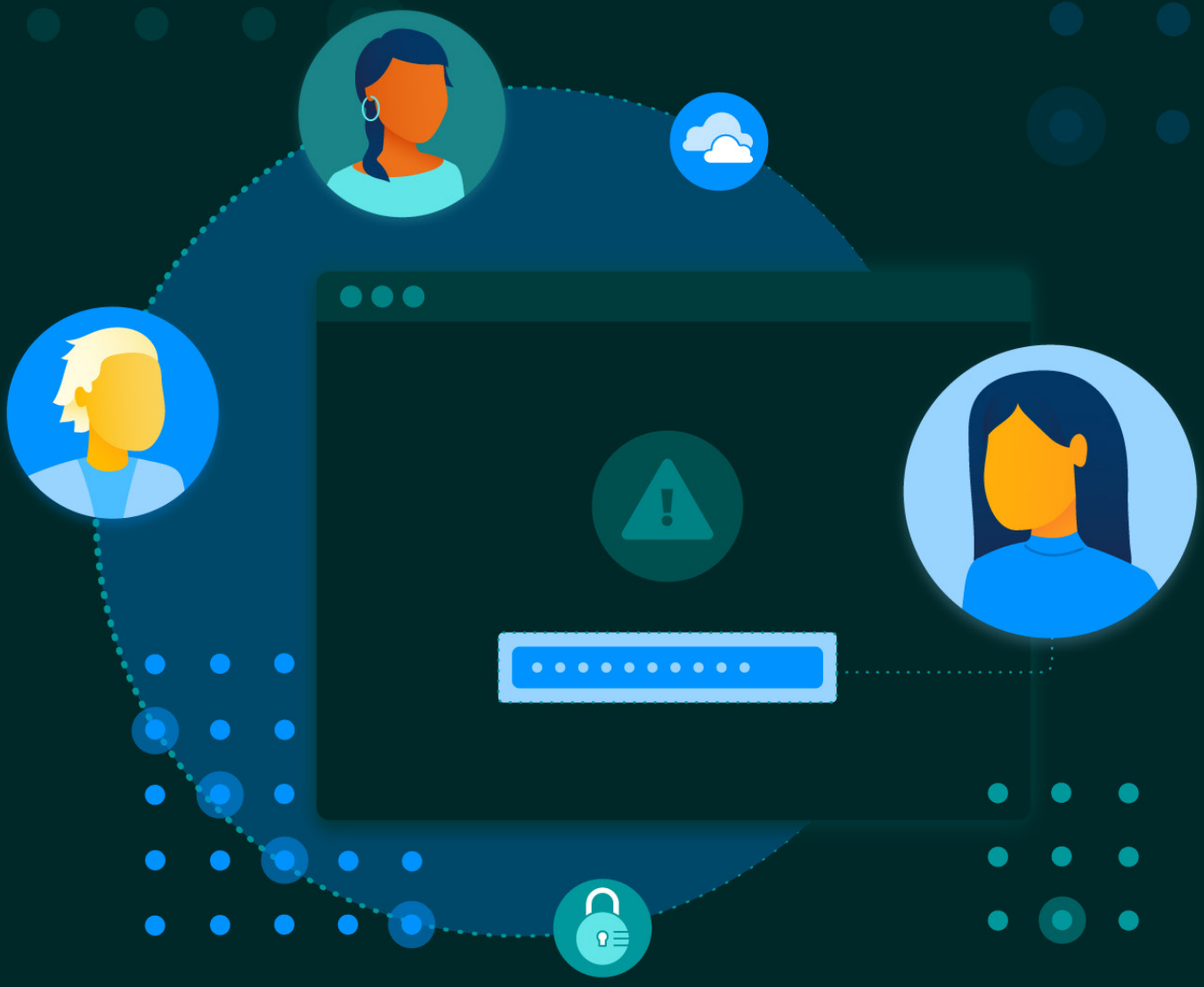
Cloud and Web Security Challenges in 2022



cloud security alliance®

Acknowledgments

Lead Author

Hillary Baron

Support

Josh Buker
Sean Heide
Alex Kaluza
John Yeoh

Special Thanks

Amanda Anderson
Joel Borgmeier
Ken Brown
Itir Clarke
Sai Chavali
Brian Gleeson
Stephanie Torto

Design

Claire Lehnert

Table of Contents

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cybersecurity in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Proofpoint commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding cloud- and web-delivered threats. Proofpoint financed the project and co-developed the questionnaire by participating with CSA research analysts. The survey was conducted online by CSA in May 2022 and received 960 responses from IT and security professionals from various organization sizes and locations. CSA's research team performed the data analysis and interpretation for this report.

Goals of the Study

The goal of this survey was to understand IT and security professionals':

- Top concerns regarding cloud and web threats
- Strategy and methods for protecting against cloud and web threats
- Current cloud governance strategies

Executive Summary

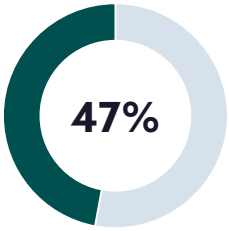
Organizations' work environments have undergone rapid but lasting changes in the face of the recent health crisis. Working remote became a necessity and many organizations were forced to accelerate their digital transformation as a result. This drastically changed the security landscape. Employees could no longer be protected by enterprise firewalls; people were becoming the new perimeter. Simultaneously, multiple newsworthy supply chain attacks occurred, drawing attention to a growing number of cloud and web attacks targeting people with access to business data. Organizations were left struggling with their new cloud environments and maintaining legacy equipment while trying to adapt their overall security strategy to the changing landscape.

Key Finding 1:

Data loss from cloud and web attacks is a top concern for organizations

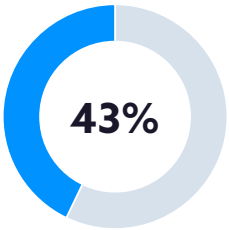
Organizations must remain constantly vigilant, preparing for and defending against potential cloud and web attacks. Attackers frequently attempt to target personal or sensitive data that can be used for their financial gain. The result for businesses can be quite extensive, including the loss of intellectual property, reputational damage, legal liability, and regulatory fines. For these reasons, data loss was ranked as the top outcome organizations are concerned about with cloud and web attacks.

Top concern regarding cloud and web attacks



Sensitive data loss/ exfiltration

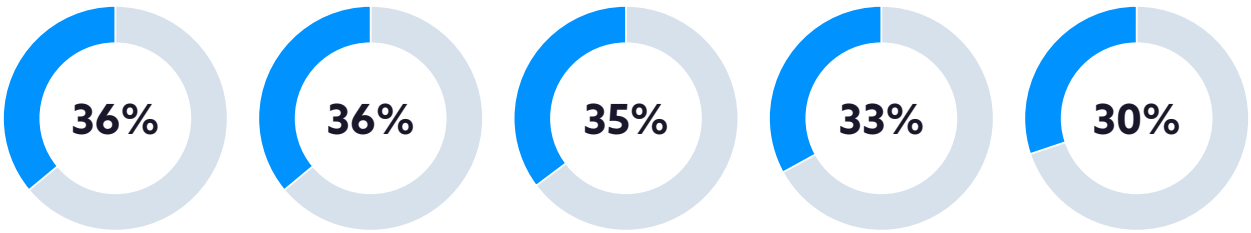
Primary cloud and web security objective for 2022



Protect customer data

The specific types of data organizations are most concerned with are customer data, credentials, and intellectual property. Forty-three percent of organizations listed protecting customer data as their primary cloud and web security objective for 2022. Organizations are concerned that targeted cloud applications either contain or provide access to data such as email (36%), authentication (37%), storage/file sharing (35%), customer relationship management (33%), and enterprise business intelligence (30%).

Types of Cloud Applications Organizations Are Most Concerned about Being Attacked



Email | Authentication platform | Storage and file sharing | Customer relationship management | Enterprise business intelligence

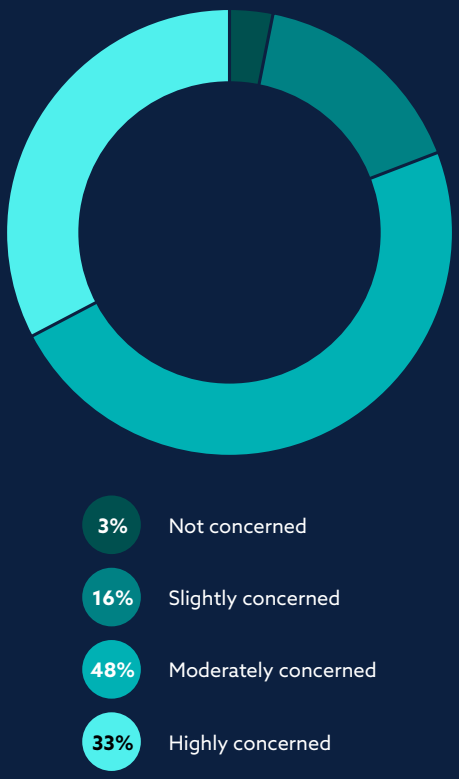
Key Finding 2:

Third parties and partners represent a high level of risk because they are most commonly the target of attacks

Risks surrounding the supply chain and third-party services have been a focus with the recent attacks on open-source solutions and the Solarwinds attack. More than **80%** of organizations are moderately to highly concerned about suppliers and partners. This high level of concern is entirely warranted as **58%** of organizations indicated that third parties and suppliers were the target of attacks. In another study by Colorado State University, 66% of breaches are the result of vulnerabilities from suppliers and third parties. Yet, as adoption of cloud computing increases, reliance on third parties and partners will only increase. Organizations must consider all parties that are dealing with sensitive data, especially third parties and partners.

Type of groups targeted in attacks

Levels of concern regarding security when collaborating with suppliers and partners

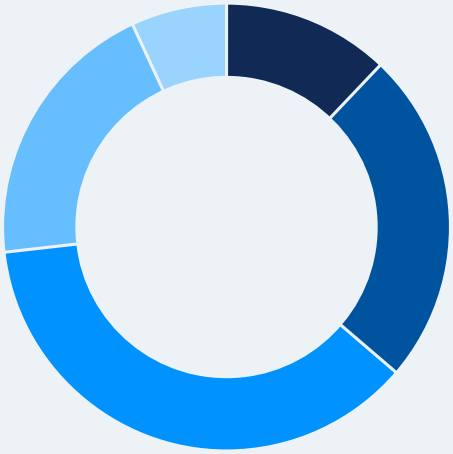


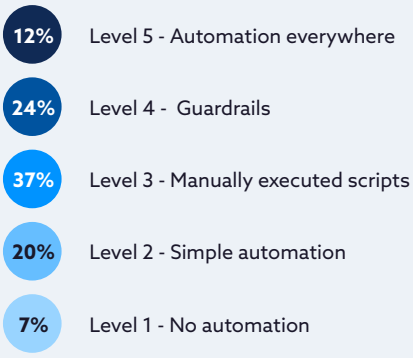
Key Finding 3:

Rapid digital transformation has left organizations struggling with their approach to cloud and web threats

On average, organizations are utilizing between three and four different solutions, but only 16% are using some form of web security to address cloud and web threats. This indicates organizations are experiencing some difficulty in how to approach this issue. The top challenge cited was the need to manage legacy and on-premises security infrastructure (47%). This can in part be attributed to the rapid pace that digital transformation initiatives were implemented to accommodate remote work during the COVID-19 pandemic. The result is a lagging cloud governance strategy. In fact, 64% of organizations rated the maturity of their cloud governance at a level three or under (based on the IANS Research Cloud Security Maturity Model). When taken together, it's clear that in their rush to enable employees for remote work, organizations' struggle to keep pace with those demands.

Maturity levels of cloud governance strategy



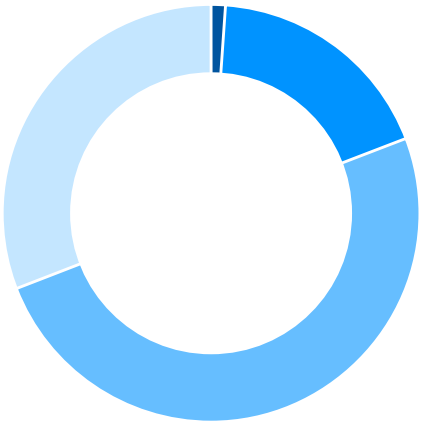


Top challenges with current solution(s) for protecting against cloud and web threats

Security Overview

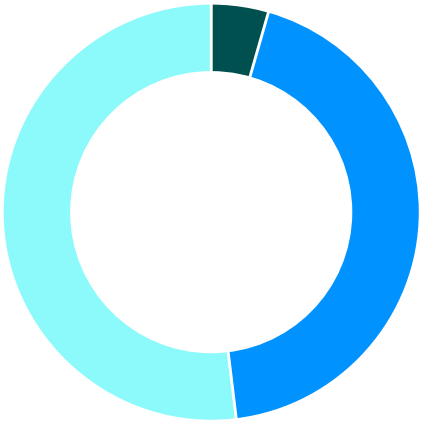
Size of cloud and web security teams

Half of the organizations surveyed have medium sized (3-9 people) cloud and web security teams. Another 31% of organizations have large teams (10+ people) and another 18% have small teams with only 1-3 people on the team.



Dedicated or cross-functional cloud security teams

These teams are most often (52%) cross-functional and not solely dedicated to cloud security. Another 44% have teams dedicated to cloud security. These organizations were most often technology and financial services firms. Only 3% report not having anyone focused on cloud security, however these organizations were primarily in non-tech industries, such as education or business support.[1]



Primary cloud and web security objectives for 2022

Protecting customer data (43%) and automating cloud and web threat prevention (41%) were the top two security objectives organizations cited for organizations in 2022. The emphasis on protecting customer data aligns with consistent concerns around data breaches and a desire to protect an organization's reputation. Automating cloud and web threat prevention is high on the list to supplement their staff as the skills gap increases and as human error continues to contribute to breaches[1].

1 Verizon DBIR. (2021). https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

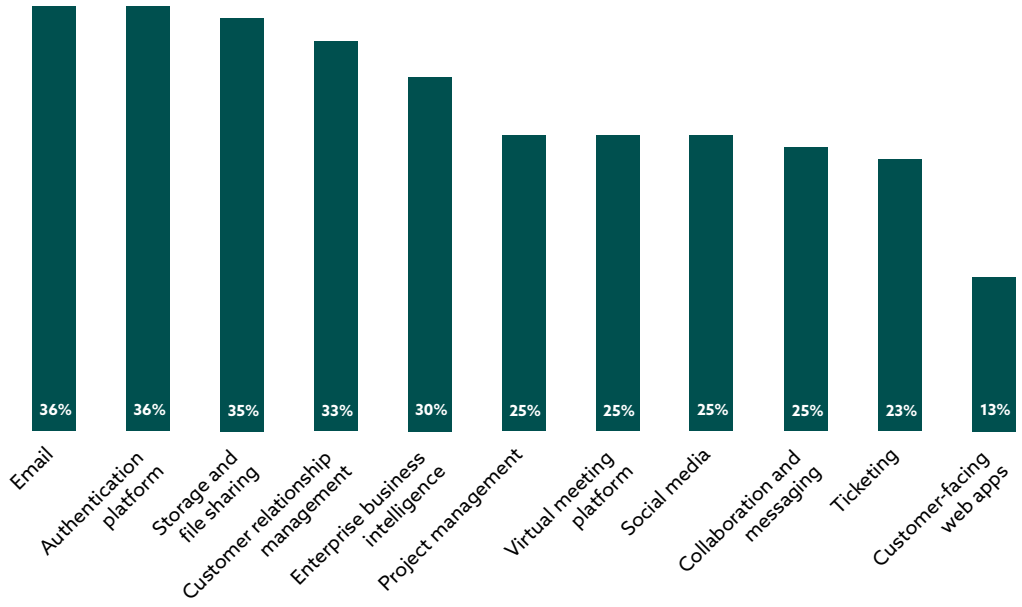
Attacks and Security Concerns

Most concerning methods of attacks

Organizations are concerned about a great many methods of attack that may target their organizations. No single type of attack appears to be of greater concern, indicating that organizations try to be vigilant for a wide array of attacks, ranging from lateral movement to privilege escalation and ransomware. However, the infiltration and expansion stages of attacks are of concern for more organizations than the later stages. Tools for detecting compromised accounts and post-compromise activity (e.g., data exfiltration, email activity) can help to ease these concerns when incorporated into their overall strategy for protecting sensitive data in the cloud.

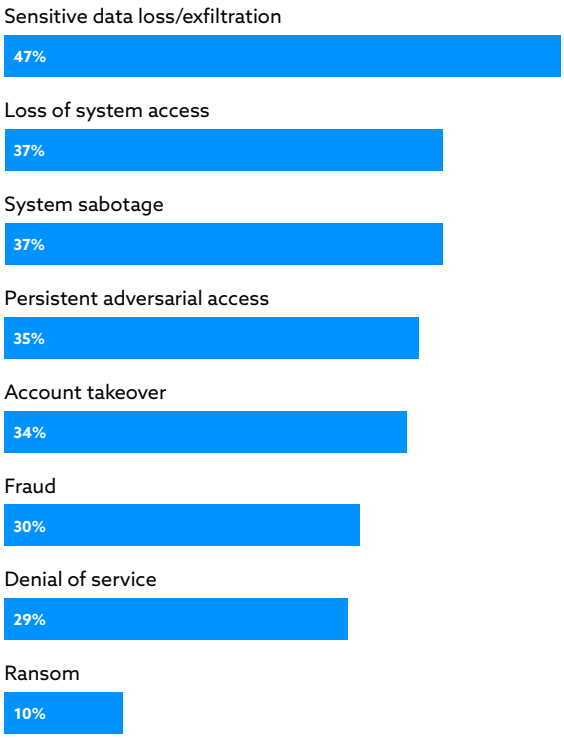
Most concerning cloud applications targeted in attacks

The types of cloud applications that organizations are most concerned about being attacked are applications that provide greater access to or contain data. The applications are also used or accessible to most employees within an organization. This is reflected in the cloud applications organizations indicated they were most concerned about being attacked. The top two concerns are when threat actors gain access to email (36%) and authentication platforms (36%). Also of significant concern were cloud applications that provide access to the organization's data, storage and file sharing (35%), customer relationship management (33%), and enterprise business intelligence (30%).



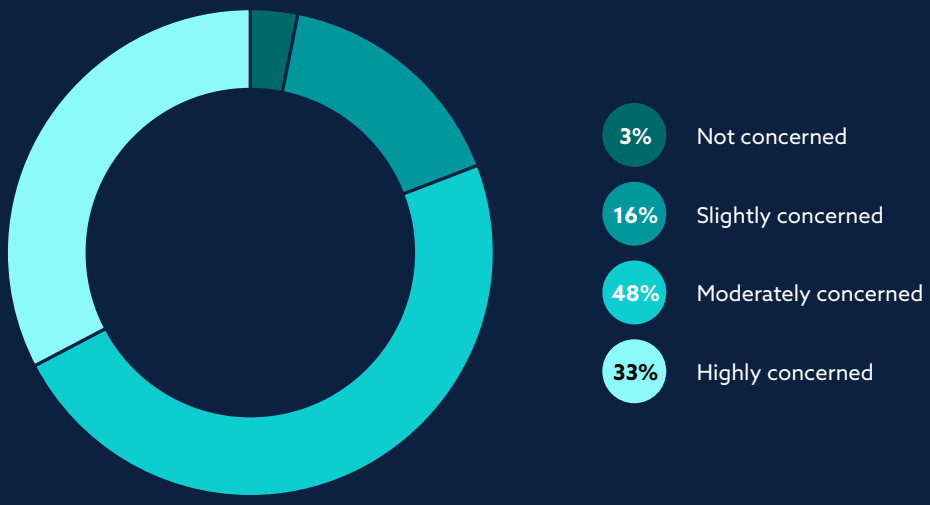
Most concerning outcomes of cloud and web attacks

The outcomes organizations are most concerned about are consistent with the types of cloud apps they see as vulnerable. The top concern is the loss of sensitive data (47%), which is likely due to the reputational, financial, and legal implications that may result from such a loss. The second most concerning outcome is around the systems themselves, including loss of system access (37%) and system sabotage (37%). The loss of system access speaks to the concerns about access previously. Concerns about system sabotage echo the concerns organizations have regarding malware and ransomware. Interestingly, paying ransoms in ransomware attacks doesn't seem to be a greater concern than the loss of data and system access.



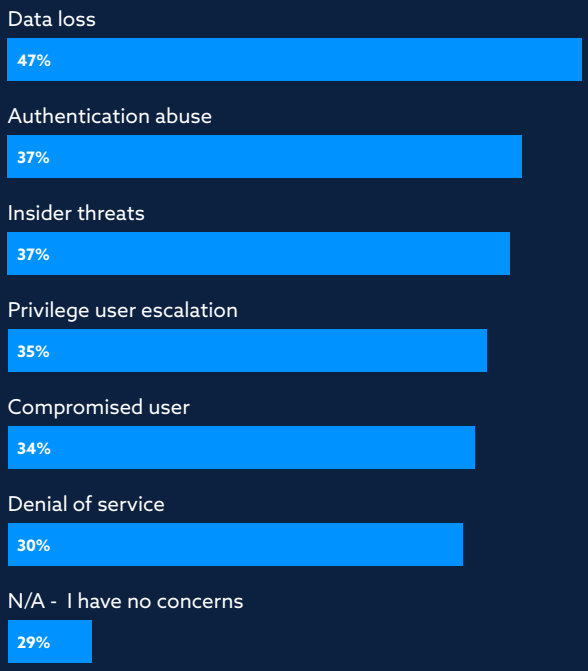
Level of concerns regarding security when collaborating with suppliers and partners

Respondents are concerned about security when collaborating with suppliers and partners. Eighty-one percent of organizations report that they are moderately or highly concerned about this issue. Once again this is consistent with recent attacks on US infrastructure and open-source solutions.



Top security concerns from partners and suppliers

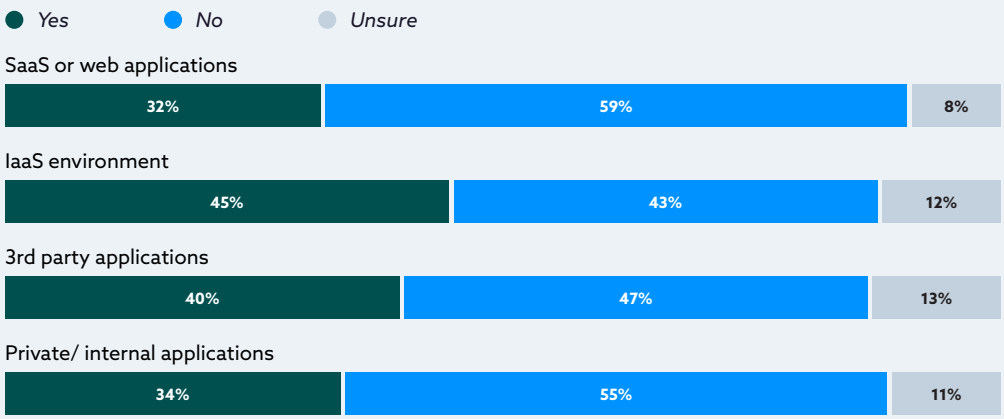
Similar to the concerns around cloud and web attack outcomes, the top security concern with partners and suppliers is data loss (48%). Regardless of the type of attack it appears that data loss, particularly sensitive data loss, is top of mind for many organizations. Authentication abuse (43%) is the second most concerning risk. This result is consistent with types of cloud applications organizations find vulnerable. These results further support the conclusion that organizations are most concerned about preventing access to data and the loss of data. Other notable concerns include insider threats (42%), privilege user escalation (40%), compromised users (39%) and denial of services (38%). Only 7% indicated they had no concerns related to their partners and suppliers.



Cloud Breaches

Cloud breaches by environment

Organizations have experienced breaches in many different environments over the past year. The results show higher levels of breaches in organizations' IaaS environment (45%) and third-party applications (40%). Fewer breaches were experienced in SaaS or web applications (32%) and private/internal applications (34%). However, it is worth noting that the 2022 Verizon Data Breach Investigation Report indicated that web applications are one of the top vectors for attacks that have increased over the past few years[2].



Groups targeted in attacks

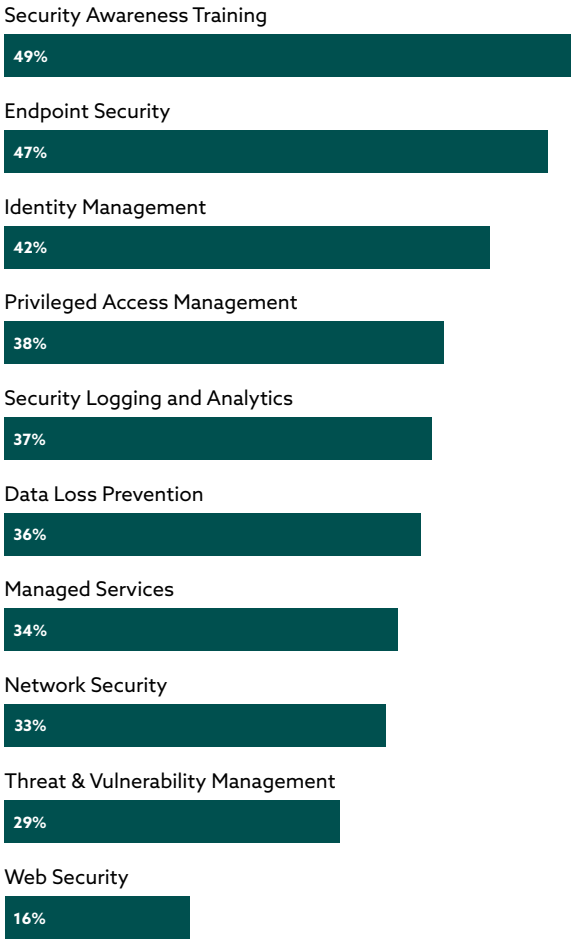
Third parties, contractors, and partners (58%) were the most targeted in cloud breaches. This is consistent with the high level of concern organizations have for security with regards to this group. The second most targeted group is customers (43%), which is consistent with organizations prioritizing protection of customer data for their cloud and web security objectives for 2022. The third most targeted group is executives and c-level employees (42%). Targeting higher management is relatively common due to their access to sensitive data. Surprisingly remote employees (35%) was one of the least commonly targeted groups among those surveyed. While they are still the target in over 33 percent of attacks, it is surprising that this group was not more commonly targeted with the high number of remote employees and decreased security.

2 2022 Data Breach Investigations Report. (2022). https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

Protecting Against Cloud and Web Threats

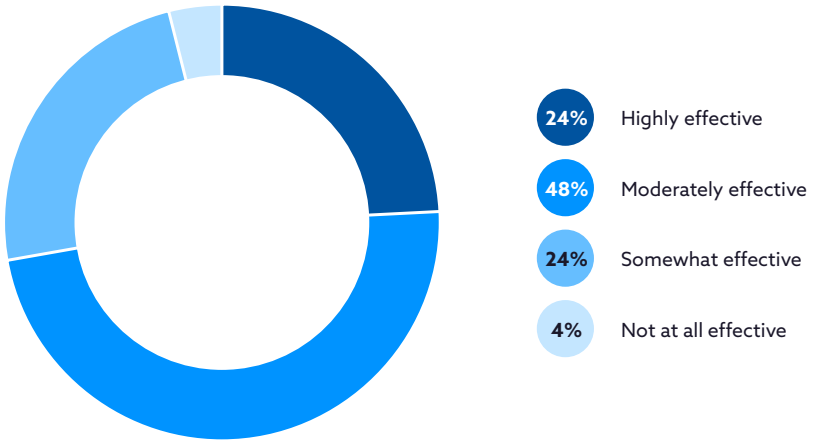
Solutions for protecting against cloud and web threats

To protect themselves against cloud and web threats, organizations' most commonly used defense is security awareness training (49%). This is a relatively simple, cost-effective method, that aims to educate employees and thereby reduce the likelihood that they will fall victim to attacks. The second most popular method is endpoint security (47%). This is likely due to the movement toward a zero trust strategy as well as the trend toward remote work. The third and fourth most popular methods are identity management solutions (43%) and privileged access management (38%). These methods are also likely due to the rise of zero trust security approaches and remote work, with many arguing that identity or people are quickly becoming the new perimeter.



Effectiveness of current cloud and web threat solutions

The methods organizations have chosen to use against cloud and web threats at present are on average moderately effective (48%). Although they are working, there is clearly still room to improve as well.



Top challenges with the current solution for protecting against cloud and web threats

The top challenges that organizations have with their current solutions are most commonly due to managing legacy and on-premises security infrastructure (47%). This is likely the result of rapid digital transformation in the face of the recent health crisis and the need for workers to work remotely. Coaching users toward more secure behavior (37%) is the second most common challenge. Although Security Awareness Training is one of the top methods for protecting against cloud and web threats, organizations appear to use it infrequently or struggle with on-going coaching after training. The third most common challenge is user productivity issues and complaints (37%). This could be the result of deficiencies in the solution, or a lack of proper training by the staff.

Most important capabilities when protecting against cloud and web threats

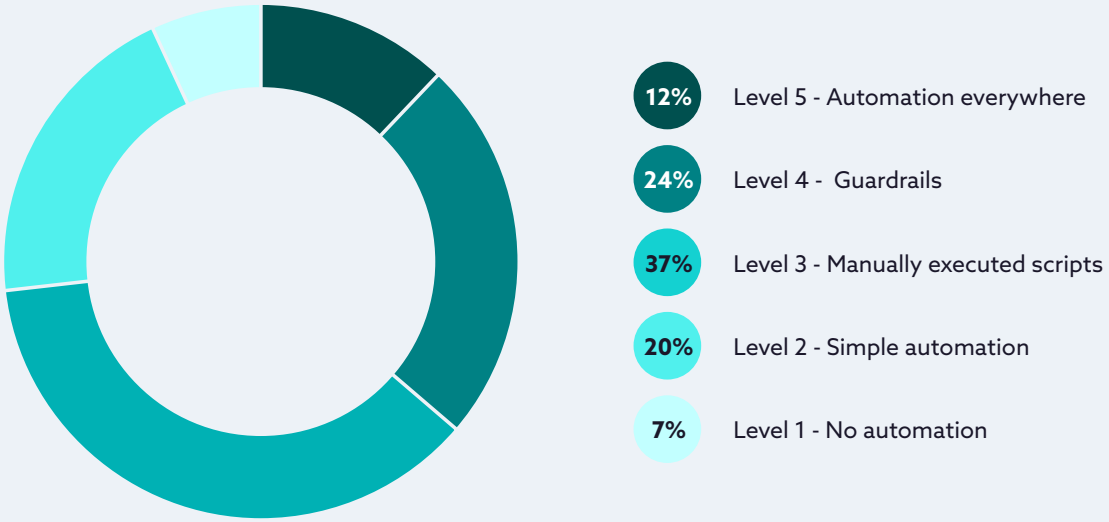
Malware prevention and detection (15%) is the capability organizations value most in their approach to protecting against cloud and web threats. This followed by account compromise detection and remediation (14%) and risk-based access controls (14%). The general pattern appears to follow an attack path.

- Malware detection & prevention
- Account compromise detection & remediation
- Visibility into misconfigurations
- Risk-based access controls
- Threat protection on unmanaged devices
- OAuth app abuse detection & controls
- Web traffic isolation/browser isolation
- Threat correlation across channels

Cloud Governance

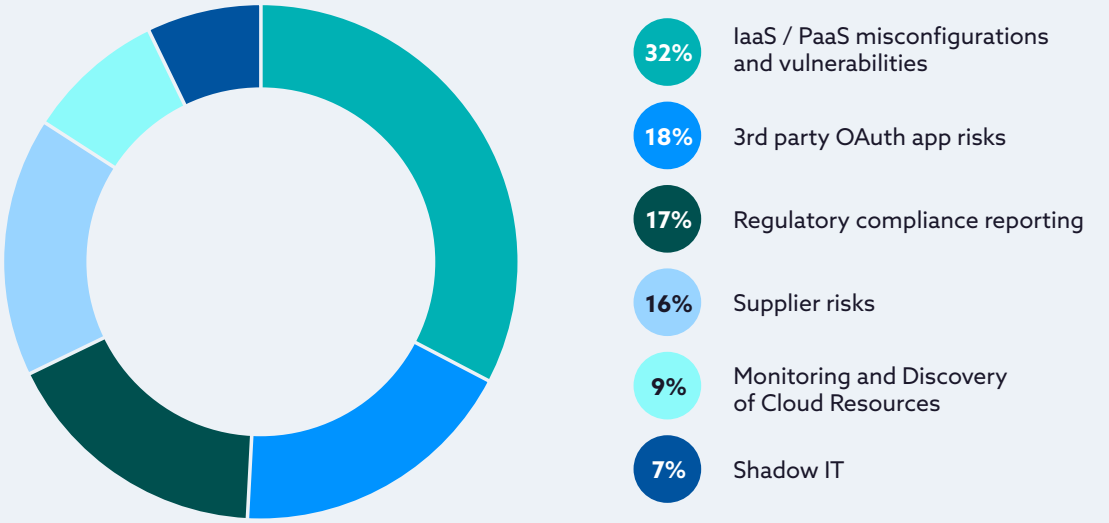
The maturity level of an organization's cloud governance

The maturity level of organization's cloud governance appears to be about mid-way to maturity. However, it is important to note that this is based on perception and is likely over-idealized.



Top challenge with cloud governance

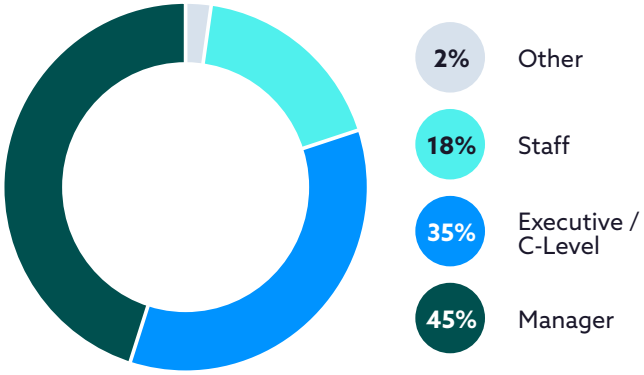
The top challenges with cloud governance for organizations are IaaS/PaaS misconfigurations and vulnerabilities (32%). This has been a top challenge and concern within the industry for several years. There are also concerns around the supply chain including third-party OAuth app risk (18%) and supplier risks (16%). This is likely due to the more recent attacks targeting the supply chain.



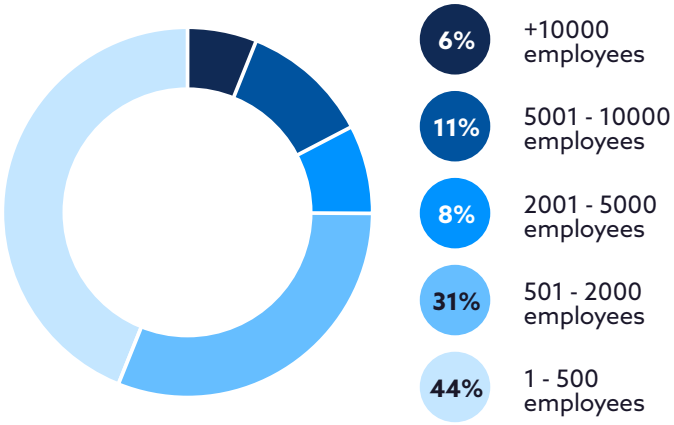
Demographics

This survey was conducted in May 2022 and gathered 960 responses from IT and security professionals from various organization sizes, industries, locations, and roles.

What is your job role?



What is the size of the organization you work for?



What region are you located in?