
orca
security
2022 Cloud Security
Alert Fatigue Report
The scale of public cloud alert fatigue, its causes,
impacts, and possible solutions
aws

Inside This Report

Executive Summary

Security professionals are all too familiar with alert fatigue. They faced it in the on-prem world, and now they're dealing with it in the cloud. Organizations use many different security tools that each generate alerts, overwhelming security teams who have to spend hours each day reviewing alerts to determine which issues need to be fixed first.

Like the story of 'The Boy Who Cried Wolf', if the amount of meaningless and false positive alerts becomes too great, responders become desensitized, resulting in alerts that actually do deserve attention, getting missed.

Executive Summary

The Survey

To find out more about the current state of alert fatigue, its causes, impacts, and possible solutions, Orca Security commissioned a global survey held among 813 IT decision makers in five countries and across ten industries.

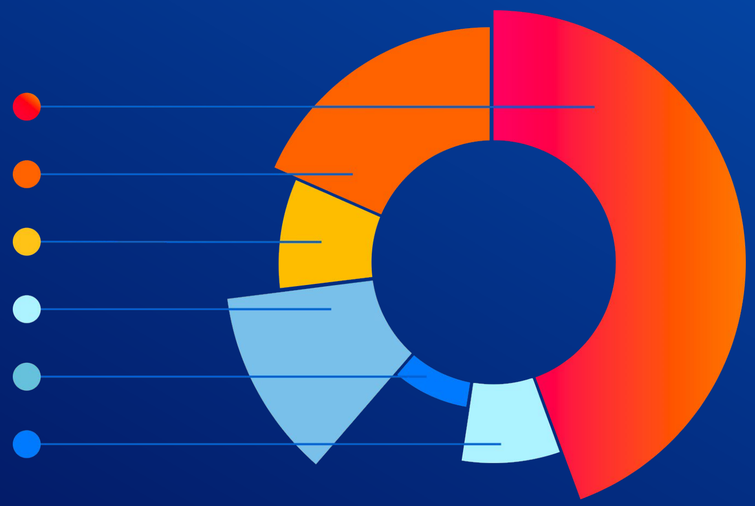
This report discusses the global findings. The key findings per country and industry are listed in the Appendix.

> The majority of respondents were from companies with **200-1,000 employees** (79%).
>
> Most respondents' cloud security teams ranged from **1 to 50 members**.

Countries

- 40% United States
- 20% Australia
- 14% Germany
- 13% France
- 13% United Kingdom

Industry



- Technology 45%
- Other 15%
- Financial 12%
- Manufacturing/CPG 11%
- Professional Services 9%
- Healthcare 8%

Executive Summary

The Respondents

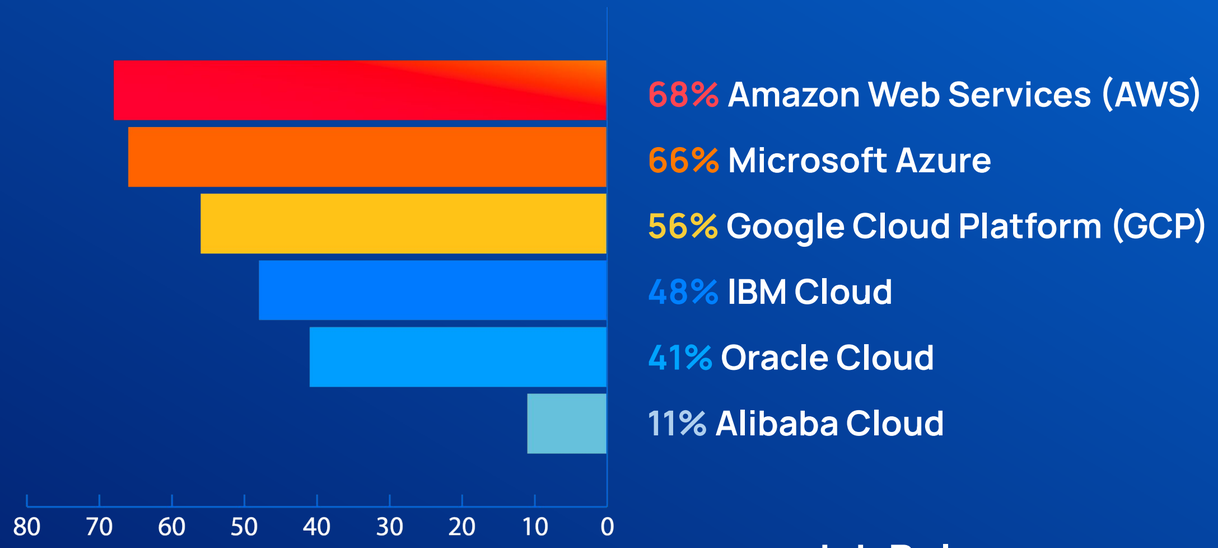
To participate in the survey, respondents needed to have at least 25 cloud assets on one of the major public cloud platforms. The majority of respondents (84%) had more than 100 cloud assets. Most respondents use AWS, Azure and Google Cloud, closely followed by IBM Cloud and Oracle Cloud.

Respondents' job levels varied from staff (10%), manager (61%), to executive (29%).

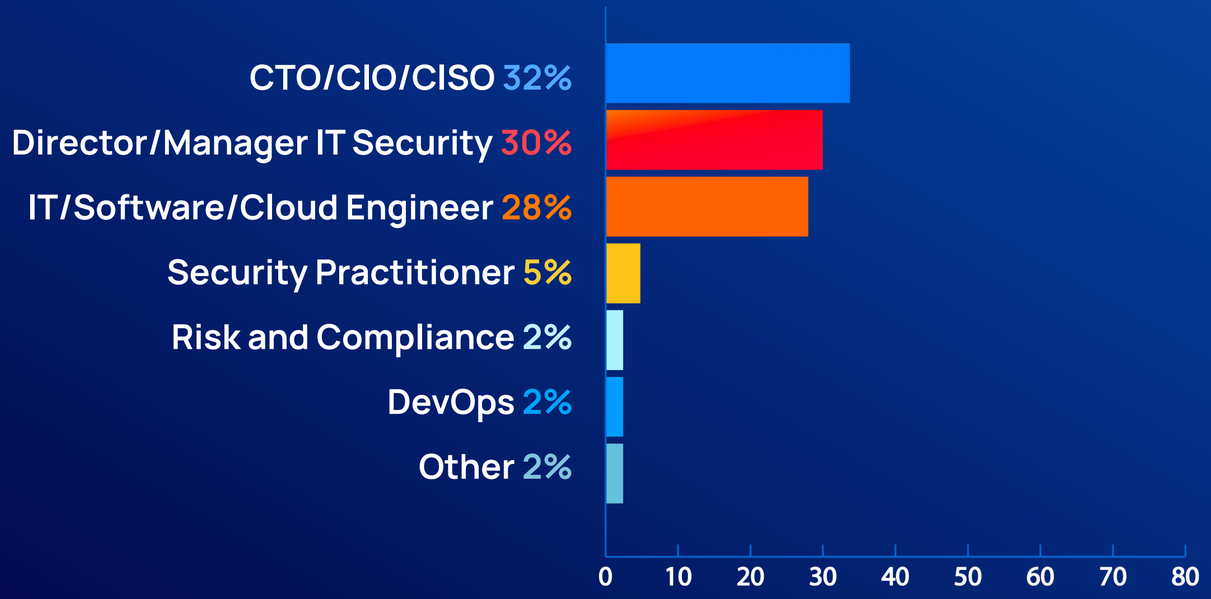
> The vast majority (81%) use a **multi-cloud strategy** with more than one cloud platform.

> 55% of respondents use **3 or more** public cloud platforms.

Public Cloud Platforms Used



Job Role



Executive Summary

Key Findings

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 59% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 43% say more than 40% of their alerts are false positives and 49% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 56% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 62% of respondents say that alert fatigue has contributed to turnover, and 60% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 55% of respondents who say that critical alerts are being missed, 41% said alerts are being missed on a weekly basis, and 22% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 57% have **5 or more public cloud security tools**.
- 95% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 43% say more than 40% of their alerts are false positives.
- 97% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 49% say that more than 40% of alerts are low priority.

59%

receive more than
500 cloud security alerts per day

62%

say alert fatigue
has contributed to turnover

95%

feel confident in the
accuracy of their security tools?

1

Security Teams Are Flooded with Alerts

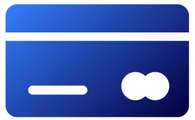
Security teams are flooded with alerts every day. 59% of respondents receive more than 500, and 38% receive more than 1,000 public cloud security alerts per day. In addition to receiving new alerts, teams also need to manage alerts that are still being remediated and have not yet been closed. 79% of respondents said they have more than 500 cloud security alerts open at any given time, and 55% said they have more than 1,000 open.

A large part of a security practitioner's day is spent reviewing and prioritizing alerts. More than half of security teams said they spend more than 20% of their time, and a quarter of teams spend more than 40% of their time deciding which alerts should be dealt with first.

A Day in the Life of a Security Practitioner:

- **59%** receive more than 500 cloud security alerts per day
- **56%** spend more than 20% of their day reviewing and prioritizing alerts
- **79%** have more than 500 cloud security alerts open on a daily basis

The Financial Industry Suffers the Most



71% of financial services respondents receive more than 500 public cloud security alerts per day, **85%** have more than 500 public cloud security alerts open, and **63%** of security teams spend more than 20% of their time reviewing and prioritizing alerts each day. This indicates that security and compliance controls are set higher for the financial services industry.

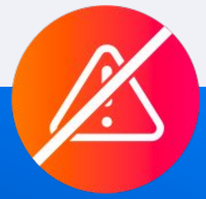
2

Alerts are Lacking in Accuracy

Security teams receive many falsely flagged issues. As many as 81% of respondents say that more than 20% of alerts are false positives. A little less than half (43%) said that more than 40% of their alerts are false positives. Regardless, teams must address each alert as if it's a true positive until they know otherwise. This leads to wasted time and contributes to desensitization.

Even if alerts are not false positives, but low priority alerts that do not need to be dealt with immediately, these still waste time if teams need to separate them from the important ones. 49% of respondents say that more than 40% of alerts are low priority and as many as 83% say that more than 20% of their alerts are low priority.

Only a small number of alerts are actually critical and need immediate attention–less than 10%, in fact, for the majority of respondents. However, to find those 10% of alerts among the hundreds of low priority and false positive alerts, teams need to spend a lot of time analyzing and investigating alerts.



The Boy Who Cried Wolf?

43%

say more than 40% of their alerts are false positives

49%

say more than 40% are low priority alerts

64%

say less than 10% of alerts are actually critical

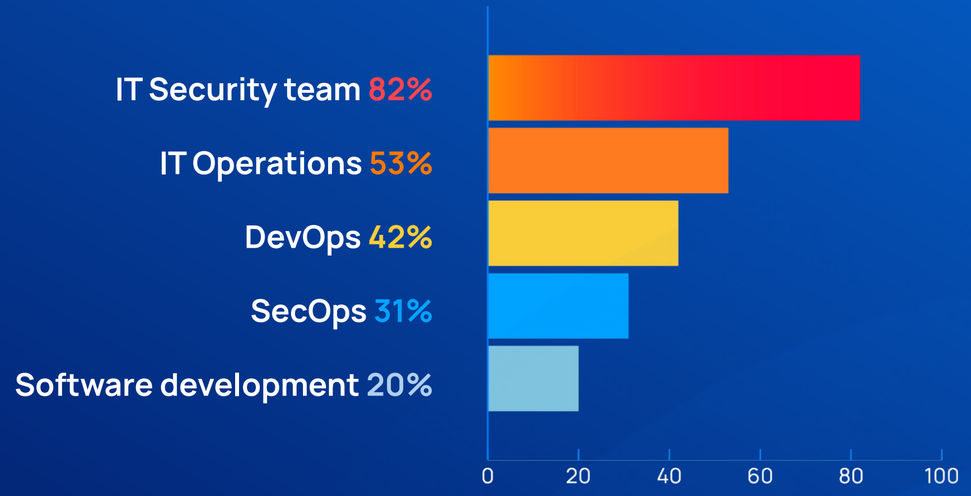
3

Remediation Burden Falls on Security Teams

In addition to deciding which alerts need to be prioritized, security teams bear the greatest responsibility for triaging and remediating alerts, with 82% of respondents listing the IT security team, and 31% listing SecOps as the group responsible for remediating alerts. Software development seems to be called upon the least often, with only 20% of respondents naming development as responsible for remediation.

Many cloud security issues are not that easy to remediate. Only 19% of respondents said that on average it takes less than one day to remediate an alert. 35% said 1-2 days, and nearly half of all respondents said that remediation takes three or more days.

Who is responsible for triaging and remediating alerts?



Security Teams Also Bear the Largest Burden of Remediation

82%
say the IT security team is responsible for remediating alerts

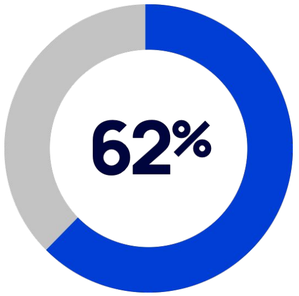
46%
said it takes 3 or more days to remediate an alert

79%
have more than 500 cloud security alerts open on a daily basis

4

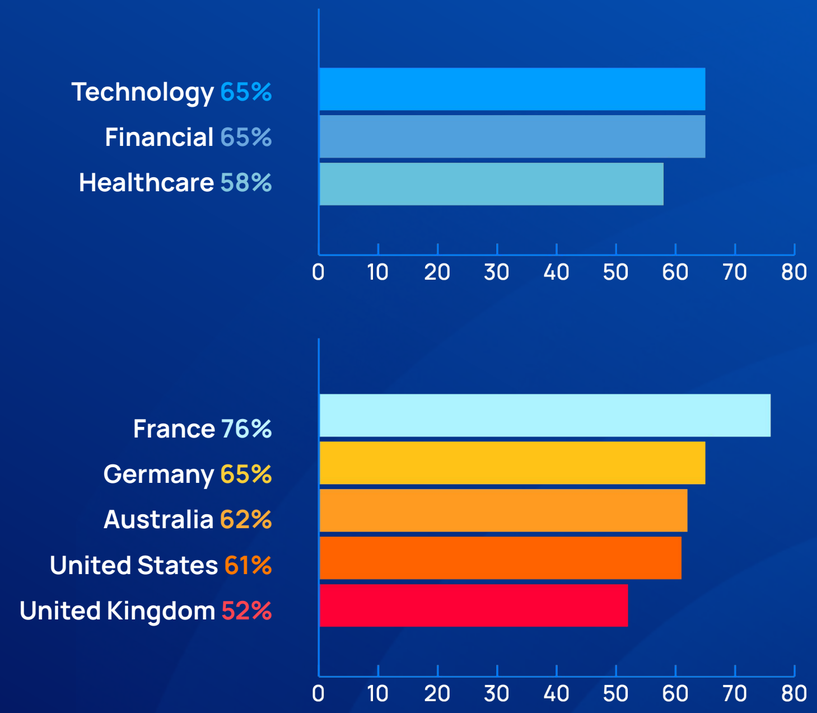
Security Teams Are Getting Burned Out

With the sheer number of alerts, with many false positives and low priority alerts and only a small number of alerts that actually need attention, teams are getting demoralized, overworked, and burned out. **62% of respondents say that alert fatigue has contributed to turnover at their organization**. No matter which country or industry, the majority of respondents all say that alert fatigue has led to staff leaving their positions. However, the UK seems to be at the lower end of the scale, and France seems to be feeling the issue the most.



of respondents say that alert fatigue has contributed to turnover at their organization.

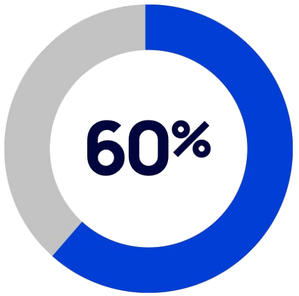
The majority say that alert fatigue has contributed to turnover:



5

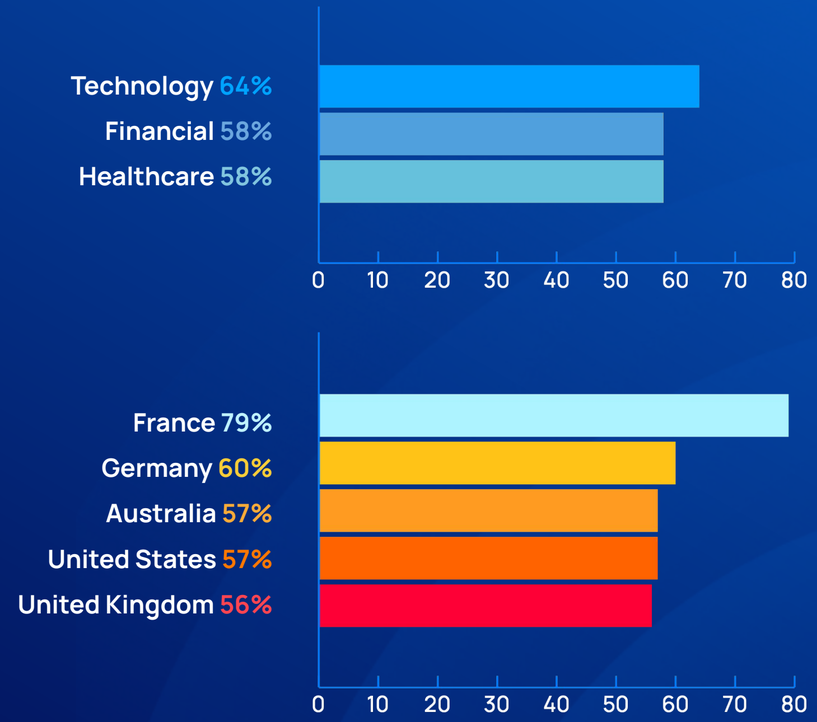
Alert Fatigue is Leading to Internal Friction

Since alert remediation is often a shared responsibility between security, IT, and DevOps, alert fatigue is also affecting internal co-operation within the organization. **60% of respondents said that alert fatigue has created friction between their DevOps and Security teams**.



of respondents said that alert fatigue has created friction between their DevOps and Security teams.

The majority say that alert fatigue has created organizational friction:



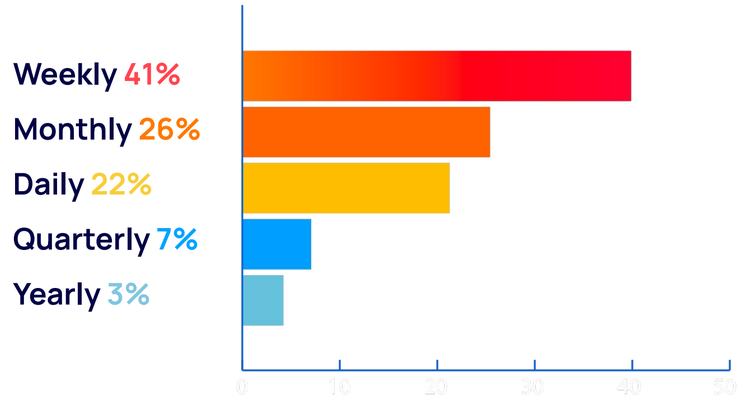
6

Critical Alerts Are Being Missed

Due to the sheer number of unprioritized alerts, security practitioners are becoming desensitized with the result that alerts that actually do need immediate attention are being missed with possibly disastrous consequences.

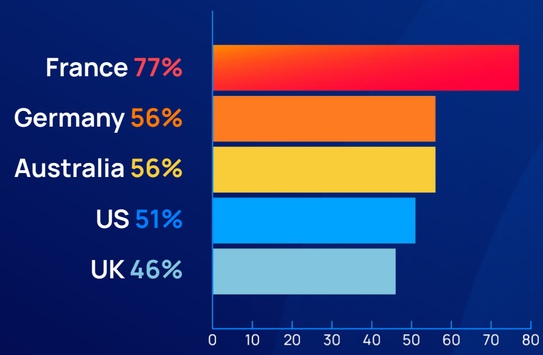
> More than half (55%) of the respondents said their team missed critical alerts in the past due to ineffective alert prioritization. Of these respondents, 22% said they missed critical alerts daily, 41% said weekly, and 26% said monthly.

Critical alerts frequently getting overlooked

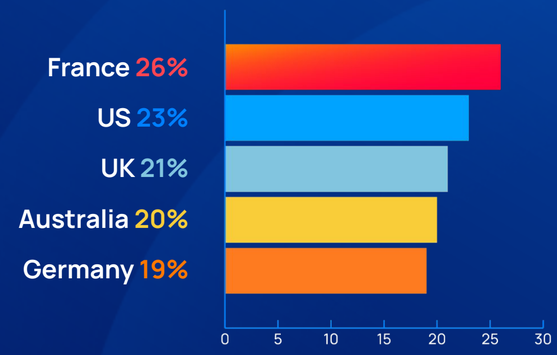


By Country

Missed critical alerts:



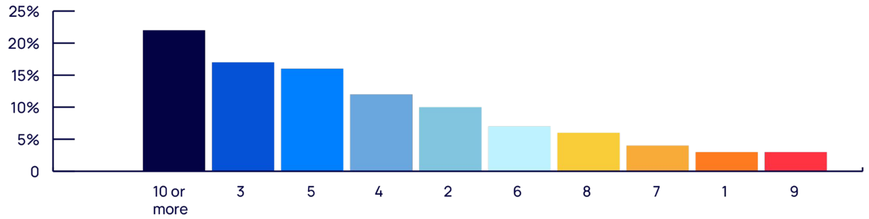
Missed critical alerts daily:



7

Siloed Security Tools Exacerbating the Problem

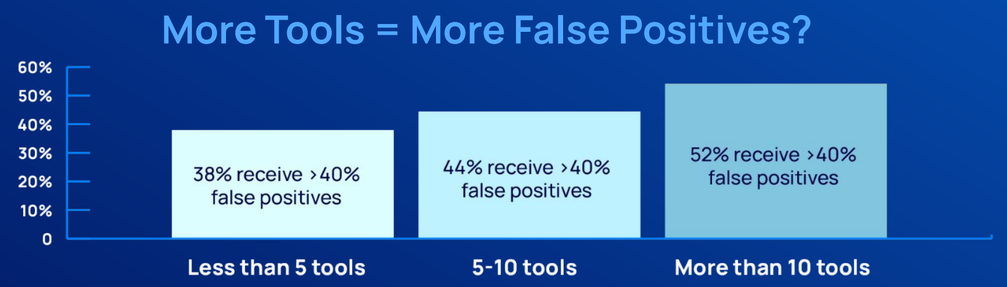
The vast majority of respondents use three or more public cloud security tools (87%), with 57% using 5 or more tools. The types of tools most used are network scanning tools (84%), followed closely by cloud platform native security tools (82%).



Number of Public Cloud Security Tools

The data shows that the more tools security teams deploy, the more alerts they receive. Part of this correlation can be explained by the fact that larger companies tend to have more security tools, and probably also have more cloud assets that alerts are generated for. However, undoubtedly another contributing factor is that multiple tools are reporting some of the same issues.

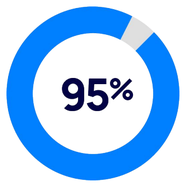
Interestingly, the proportion of false positives also seems to increase the more tools you have, as well as the alert fatigue problem, which seems to again point to the fact that multiple tools are reporting the same issues, creating duplicate work for security teams.



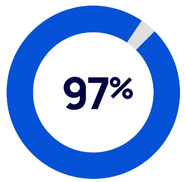
8

Is the Bar For Security Tools Being Set Too Low?

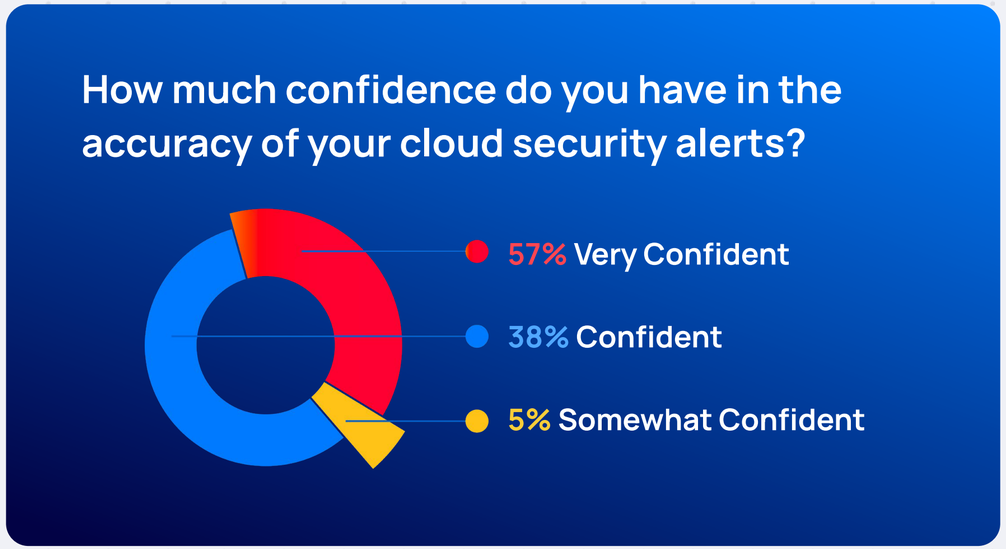
The overwhelming majority of respondents express satisfaction and confidence in the alert prioritization and accuracy of their security tools. However, our research shows that this confidence may not be fully earned. Are our respondents setting the bar too low?

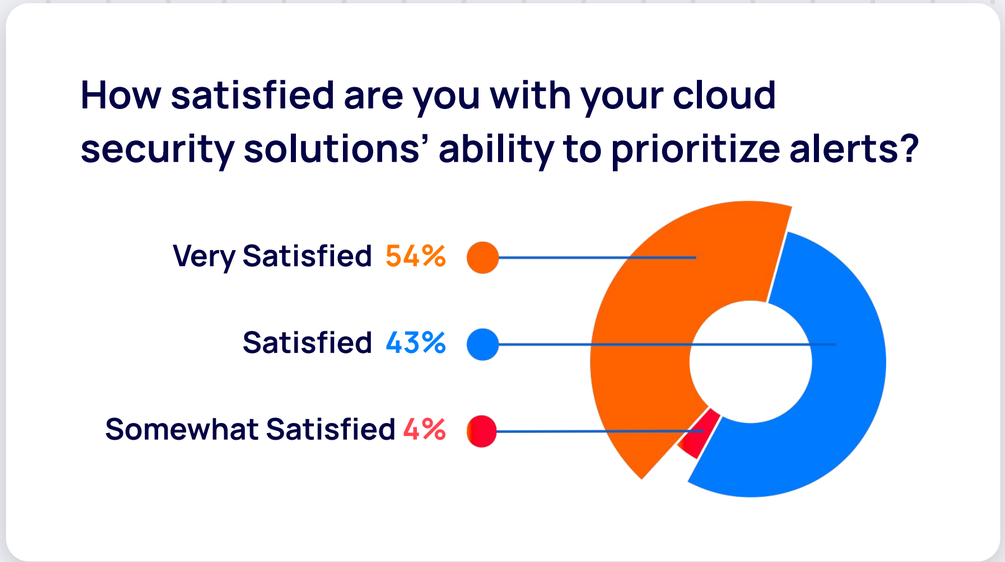


95% of respondents say they feel confident or very confident in the accuracy of their security tools, however 43% say more than 40% of their alerts are false positives.



97% of respondents say they are satisfied or very satisfied with how their security tools prioritize risk, even though 49% say that more than 40% of alerts are low priority.





9

Key Recommendations

The survey shows that alert fatigue is a major problem in most cloud security teams. Not only is this leading to staff turnover, but it is also resulting in missed critical alerts, often on a weekly or even daily basis. The use of multiple siloed tools to report cloud security alerts is creating duplicate alerts and unnecessarily increasing the burden on already overworked security teams.

So what can organizations do to address the alert fatigue problem? Organizations need to empower security teams to work smarter, not harder.

Tool consolidation: Instead of adding more siloed tools, consolidate tools in fewer platforms to avoid duplicated alerts and improve risk prioritization by leveraging centralized contextual information to discover dangerous risk combinations.

Demand more from your security tools: Ask security vendors how they prioritize risk. Ensure that they combine numerous factors such as severity, ease of exploitation, accessibility and potential business impact.

Protect the target instead of the entry point: Make sure you know where your most critical assets are, and find out if your security vendor automatically prioritizes risks based on potential exposure of these assets.

Focus on attack paths: Security teams need to shift from investigating siloed alerts to investigating and prioritizing attack chains to get quicker insight into which issues need to be fixed first.

Strategic remediation: Instead of trying to fix all alerts in the attack chain, start by fixing the one that breaks the chain to stem the most immediate danger.

Appendix

Key Findings
US

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 61% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 48% say more than 40% of their alerts are false positives and 54% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 63% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 61% of respondents say that alert fatigue has contributed to turnover, and 57% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 51% of respondents who say that critical alerts are being missed, 37% said alerts are being missed on a weekly basis, and 23% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 58% have **5 or more public cloud security tools**.
- 95% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 48% say more than 40% of their alerts are false positives.
- 96% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 54% say that more than 40% of alerts are low priority.

61%

receive more than
500 cloud security alerts per day

61%

report alert fatigue
has contributed to turnover

95%

feel confident in the
accuracy of their security tools?

Key Findings
UK

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 53% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 45% say more than 40% of their alerts are false positives and 54% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 52% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 52% of respondents say that alert fatigue has contributed to turnover, and 56% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 46% of respondents who say that critical alerts are being missed, 46% said alerts are being missed on a weekly basis, and 21% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 60% have **5 or more public cloud security tools**.
- 91% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 43% say more than 40% of their alerts are false positives.
- 96% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 54% say that more than 40% of alerts are low priority.

53%

receive more than
500 cloud security alerts per day

52%

report alert fatigue
has contributed to turnover

91%

feel confident in the
accuracy of their security tools?

Key Findings
France

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 61% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 40% say more than 40% of their alerts are false positives and 43% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 45% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 76% of respondents say that alert fatigue has contributed to turnover, and 79% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 77% of respondents who say that critical alerts are being missed, 40% said alerts are being missed on a weekly basis, and 26% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 60% have **5 or more public cloud security tools**.
- 99% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 40% say more than 40% of their alerts are false positives.
- 97% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 43% say that more than 40% of alerts are low priority.

61%

receive more than
500 cloud security alerts per day

76%

report alert fatigue
has contributed to turnover

99%

feel confident in the
accuracy of their security tools?

Key Findings
Germany

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 54% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 41% say more than 40% of their alerts are false positives and 48% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 50% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 65% of respondents say that alert fatigue has contributed to turnover, and 60% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 56% of respondents who say that critical alerts are being missed, 54% said alerts are being missed on a weekly basis, and 19% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 43% have **5 or more public cloud security tools**.
- 95% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 41% say more than 40% of their alerts are false positives.
- 96% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 48% say that more than 40% of alerts are low priority.

54%

receive more than
500 cloud security alerts per day

65%

report alert fatigue
has contributed to turnover

95%

feel confident in the
accuracy of their security tools?

Key Findings
Australia

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 61% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 36% say more than 40% of their alerts are false positives and 42% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 56% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 62% of respondents say that alert fatigue has contributed to turnover, and 57% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 56% of respondents who say that critical alerts are being missed, 39% said alerts are being missed on a weekly basis, and 20% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 61% have **5 or more public cloud security tools**.
- 94% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 36% say more than 40% of their alerts are false positives.
- 97% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 42% say that more than 40% of alerts are low priority.

61%

receive more than
500 cloud security alerts per day

62%

report alert fatigue
has contributed to turnover

94%

feel confident in the
accuracy of their security tools?

Key Findings

Financial Service Global

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 71% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 42% say more than 40% of their alerts are false positives and 51% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 63% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 65% of respondents say that alert fatigue has contributed to turnover, and 58% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 61% of respondents who say that critical alerts are being missed, 35% said alerts are being missed on a weekly basis, and 25% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 58% have **5 or more public cloud security tools**.
- 91% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 42% say more than 40% of their alerts are false positives.
- 94% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 51% say that more than 40% of alerts are low priority.

71%

receive more than
500 cloud security alerts per day

65%

report alert fatigue
has contributed to turnover

91%

feel confident in the
accuracy of their security tools?

Key Findings
Healthcare Global

Alert Fatigue by the Numbers:

- **Security teams are inundated with cloud security alerts:** 53% of respondents receive more than 500 cloud security alerts per day.
- **A large number of alerts are inaccurate or unnecessary:** 32% say more than 40% of their alerts are false positives and 45% say more than 40% of alerts are low priority.
- **Reviewing and prioritizing alerts is a major task:** 48% spend more than 20% of their day reviewing alerts and deciding which ones should be dealt with first.

Alert Fatigue Causes Turnover and Missed Critical Alerts:

- **Alert fatigue causes burnout, turnover, and internal friction:** 58% of respondents say that alert fatigue has contributed to turnover, and 58% said that alert fatigue has created internal friction.
- **Critical alerts are being missed, often on a daily and weekly basis:** Of the 48% of respondents who say that critical alerts are being missed, 41% said alerts are being missed on a weekly basis, and 34% said on a daily basis.

Is The Bar For Security Tools Being Set Too Low?

- 53% have **5 or more public cloud security tools**.
- 97% of respondents say they feel **confident or very confident in the accuracy** of their security tools, even though 32% say more than 40% of their alerts are false positives.
- 97% of respondents say they are **satisfied or very satisfied with how their security tools prioritize risk**, even though 45% say that more than 40% of alerts are low priority.

53%

receive more than
500 cloud security alerts per day

58%

report alert fatigue
has contributed to turnover

97%

feel confident in the
accuracy of their security tools?

About Orca Security

Orca Security provides instant-on security and compliance for AWS, Azure, and GCP — without the gaps in coverage, alert fatigue, and operational costs of agents or sidecars. Simplify cloud security operations with a single CNAPP platform for workload and data protection, cloud security posture management (CSPM), vulnerability management, and compliance.

Orca Security prioritizes risk based on the severity of the security issue, its accessibility, and business impact. This helps you focus on the critical alerts that matter most. Orca Security is trusted by global innovators, including Databricks, Autodesk, NCR, Gannett, and Robinhood.

Connect your first account in minutes:
https://orca.security or take the free cloud risk assessment.