THE IMPACT

CLOUD RISK EXPOSURE 2025

ZEST

WWW.ZESTSECURITY.IO

FORWARD

Before we dive in...

We conducted a comprehensive survey to better understand the challenges security teams face and the connection between incidents and remediation. As part of this effort, we interviewed over 150 security decision makers working in large U.S. enterprises.

One key finding is that **62% of incidents are related to risks already known to the organization** — meaning the security team had previously identified the issue and had an open ticket for remediation when the incident occurred. This highlights the adverse impact of remediation delays and aligns with a broader trend we're observing. As there is more pressure to close tickets and resolve issues quickly to reduce the number of incidents, **SecOps teams are becoming more involved in cloud and application risk management, with the process being treated with the same urgency seen in incident response.**

Snir Ben Shimol
CEO & Co-Founder
ZEST Security

KEY FINDINGS

1 Most incidents are tied to risks known to the organization.

Over 62% of incidents originate from risks that the security team had previously identified, researched fixes for, and had open tickets for remediation in the backlog.

2 Remediation takes months, attackers only need days.

Organizations reported that it takes 10X longer to remediate vulnerabilities than it does for attackers to exploit them, highlighting a significant attacker advantage.

3 The true cost of remediation is staggering.

The annual operational costs of remediation, based on the time, resources, and effort reported by respondents, amounts to over $2 million dollars. This excludes additional indirect costs as a result of incidents, insurance, and regulatory requirements.

4 Organizations are shifting focus to reduce cloud incidents.

Now that security teams have adequate visibility into cloud risks, the focus has shifted to implementing new processes and programs that drive efficient remediation. **Survey respondents highlighted effort-based prioritization, automation, and mitigating controls** as critical components of these programs.

1

Most Incidents are Related to Risks Known to the Organization

The high volume of alerts, combined with tedious and manual remediation processes, has security teams constantly fighting an ever-growing risk backlog. As a result, an increasing number of incidents are directly related to risks known to the organization – meaning the security team was previously aware of the issue and had an open ticket for remediation when the incident occurred, but the fix had not been implemented.

> "In my experience leading incident response teams, I've found that in nearly every case, the vulnerability or misconfiguration used to gain initial access was something the security team already knew about. For some reason, though, it wasn't fixed – maybe it was de-prioritized because it required too much effort to remediate, there was no patch available, or the system was too outdated to upgrade."

Mor Levi
VP Security
Salesforce

OVER

62%

of incidents are related to previously identified risks already in the backlog, according to nearly half of respondents.

WHAT CONTRIBUTED TO THIS?

56%

of risks cannot be remediated, according to nearly half of respondents.

Risks without a clear remediation path are often accepted by the organization i.e. "acceptable risk", increasing the potential for security incidents when appropriate mitigating controls are not implemented.

87%

reported a typical backlog of over **100 critical security tickets.**

55

tickets opened per month, according to 71% of organizations

10

tickets closed per month, according to 45% of organizations

*A ticket is a record created when a security risk or vulnerability has been identified. It includes details of the issue, including a propsed fix, and is assigned to the relevant owner or team for resolution.

Visibility ≠ Security

Knowing about your problems is only step one. These statistics highlight that visibility alone is not enough — organizations require a more effective approach to remediation and mitigation to reduce cloud incidents.

2

Remediation Takes Months, Attackers Only Need Days

Today security teams are struggling to efficiently remediate cloud security risks. The process is extremely manual, time consuming, and in some cases, impossible.

While it takes security teams months to remediate vulnerabilites, it only takes attackers days to exploit them. According to Mandiant, the average time-to-exploit (TTE) is now just 5 days (compared to 32 days the previous year), highlighting the accelerating pace at which attackers are evolving compared to defenders.

10X

On average, it takes organizations 10X longer to remediate open vulnerabilities than it takes attackers to exploit them.

Breaking down MTTR

Prioritization and analytics

6-8 working days
The time a security engineer spends each month reviewing, validating, and prioritizing risks, according to 43% of respondents.

Remediation efforts

3.5 weeks
is the time to remediate a misconfiguration in production, according to 48% of respondents.

6 weeks
is the time to remediate an application vulnerability in production, according to 38% of respondents

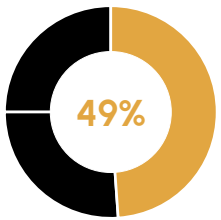
Over 8 weeks
is the time to remediate an application vulnerability in production, according to 26% of respondents.

60%

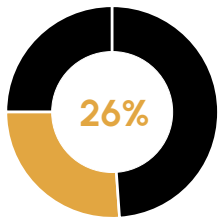
Reported that container and application security risks are the most painful to remediate.

Second most painful was cloud misconfigurations and cloud infrastructure as code (IaC) remediations.

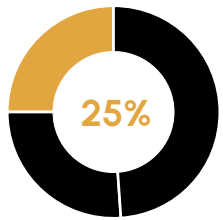
Top challenges increasing MTTR, according to survey respondents.



said understanding the best path for resolution (patch, code change, mitigating controls)



said risks that cannot be remediated (e.g. no patch available, legacy system, too much of an effort, etc.)



said the amount of time and effort required from other departments

"In the cloud, it's all about configurations. An exposed S3 bucket, for example, is much faster to exploit than a CVE. The cloud's complexity has created new opportunities for attackers to efficiently execute critical stages of an attack."

Vladi Sandler
Director of Integrations
Cisco

The True Cost of Remediation is Staggering

While difficult to quantify, the insights from this survey can help us better understand the cost of remediation. By focusing solely on direct operational expenses – excluding both incident-related costs and missed opportunities while teams focus on manual remedation tasks (instead of strategic or revenue-generating initiatives e.g. product development or scalability) — we can estimate the annual operational costs associated with remediation.

OVER $2M

Estimated annual cost of remediation

Time Invested

6-8
Working days per month invested in prioritization and analytics

3.5
Weeks to remediate misconfigurations

6-8+
Weeks to remediate application vulnerabilities

People Involved

87% have **more than 4 people** involved in opening and closing a security ticket.

Tickets Handled

55 opened per month

10 closed per month

"While our tools have gotten really good at identifying vulnerabilities, acting on them is extremely complex. Getting something fixed requires a lot of context that's often not readily available, close cross-team collaboration, and constant negotiation to get things prioritized – all of which drive up the cost of remediation."

Matthew Hurewitz
Director of Application Security
Best Buy

4

Shifting Focus to Reduce Cloud Incidents

The visibility problem has been solved—today's security teams know about their risks. Still, vulnerability exploitation continues to be one of the most common ways attackers gain initial access. **Visibility is not security and the focus has now shifted from visibility to action.**

Security teams are actively implementing new strategies to increase remediation efficiency, reduce risk acceptance, and minimize overall exposure.

Survey respondents highlighted these three strategies key to reducing exposure:

1. Effort-based prioritization
2. Automation
3. Mitigating controls

Security professionals are increasingly adopting **effort-based prioritization** as a strategy to address the largest number of risks with the least amount of changes, maximizing their impact on reducing the backlog.

53%

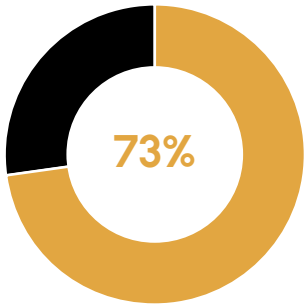
reported that prioritizing remediation based on the number of issues resolved with a single fix led to more efficient outcomes.

Mobilizing mitigating controls is gaining momentum

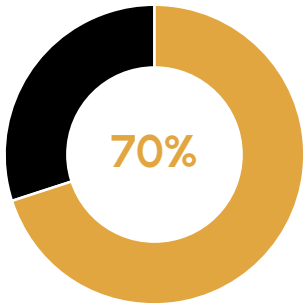
84%

research mitigating controls to reduce the risk/severity of the vulnerability when remediation is not possible. This includes leveraging cloud-native services and/or existing controls, like WAF, to reduce risk.

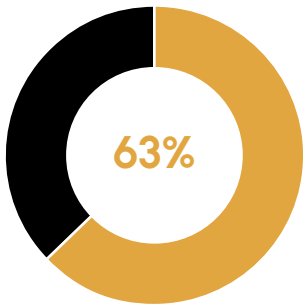
Top activities respondents wish to automate to reduce security tax and debt



wish to automate triage and root cause analysis



wish to automate identifying where and who should apply the fix (the owner)



wish to automate prioritization efforts

"A clearer understanding of the effort required from engineering and platform teams to address prioritized security risks enables more effective collaboration. This improves MTTR, enhances productivity, and fosters a more streamlined remediation process."

Aaron Brown
Head of Security
Vercel

About ZEST Security

ZEST Security offers an Agentic-AI risk resolution platform that redefines cloud risk remediation for security and DevOps teams. ZEST resolution paths provide both remediation and mitigation using code and existing controls to eliminate cloud vulnerabilities and misconfigurations. With ZEST, it's not about opening tickets; it's about closing them. Backed by leading VCs, ZEST is introducing Agentic AI into security architecture and engineering. ZEST was founded in November 2023 and has offices in New York City and Tel Aviv.

For more information visit www.zestsecurity.io

Research Methodology

This survey was conducted by a global third-party research firm and surveyed 150 security decision-makers working in enterprise organizations based in the United States. To qualify for this survey, respondents had to be manager level or above, with decision-making authority in one of the following areas: security engineering, vulnerability management, product security, application security, or DevOps. Further, surveyed organizations had to have a cloud production environment and in-house development teams.

ZEST

www.zestsecurity.io