WHITE PAPER

6 Core Capabilities For Cloud Risk Resolution

ZEST

A Shift to Risk Resolution

Today security teams are struggling to efficiently remediate cloud security risks. The process is extremely manual, time consuming and in some cases, impossible. The sheer volume of risks that surface on a daily basis coupled with the lack of automation means organizations struggle to prioritize effectively and are forced to accept a significant amount of risk. Cloud risk remediation in its current state is not only costing organizations millions of dollars per year in operational spending, it has also directly contributed to a drastic increase in successful exploitation of known cloud risks.

Inefficient remediation is leading to incidents. According to Mandiant's most recent M-Trends report, vulnerability exploitation is the top initial access vector and cloud-native misconfigurations are the main enabler for adversaries to maintain access, move laterally and accomplish mission objectives. Further, Mandiant recently reported a dramatic decrease in the average time-to-exploit (TTE), now just 5 days, compared to 32 days the previous year. This highlights both the accelerating pace at which attackers are evolving and exploiting vulnerabilities, and the urgent need for security teams to respond more quickly to open risks.

It's critical that we rethink how cloud risks are handled today and implement a new, innovative approach. This is where cloud risk resolution is gaining momentum.

Risk Resolution vs. Remediation

Risk resolution redefines the way organizations handle cloud misconfigurations, vulnerabilities and other risks. Cloud risk resolution offers a three-pillar approach, delivering remediation, mitigation and prevention. By applying artificial intelligence and automation, manual overhead is eliminated, mean time to remediate (MTTR) is drastically reduced and an organization's attack surface is minimized.

The Three Pillars of Risk Resolution

Remediate

Take a code-first approach using Infrastructure as Code (IaC) that addresses the root cause of the issue. Leverage the same tools that introduced the problem to resolve it.

Mitigate

Remediation isn't always possible. Leverage existing cloud-native controls and services to reduce risk until a full fix can be implemented.

Prevent

Ensure today's fixes solve tomorrow's problems. Prevent future and recurring risks natively in your CI/CD process without disrupting business continuity.

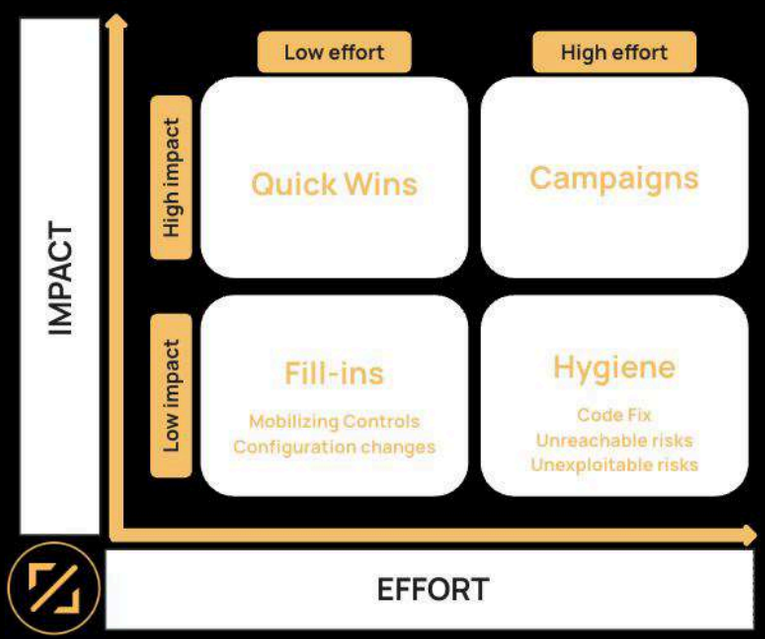
This white paper outlines the six core capabilities for cloud risk resolution, which are essential in making the end-to-end risk remediation and mitigation process more efficient and effective.

1. Effort-Based Prioritization
2. Automated Root Cause Analysis
3. Artificial Intelligence (AI)
4. Security as Code (SaC)
5. Mitigation Paths
6. Remediation Validation

Core Capability #1

Effort-Based Prioritization

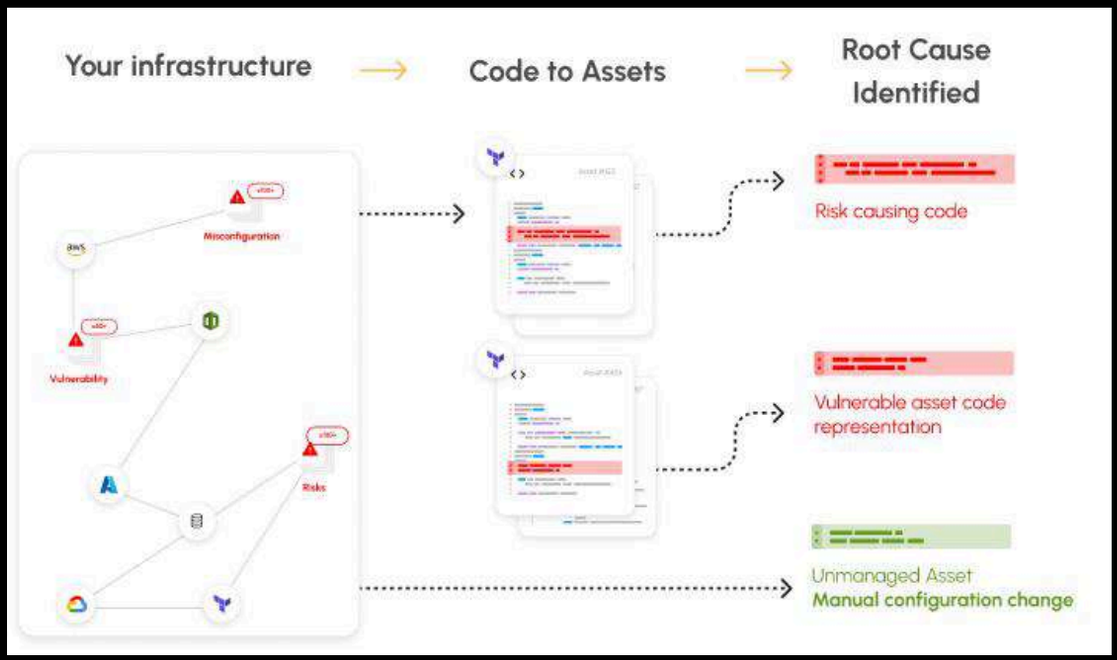
A big challenge for security teams is that they are constantly up against an ever-growing backlog of risks, while struggling to prioritize effectively. On average, organizations identify hundreds of new critical risks daily. With current approaches, this is far beyond what any security team could possibly manage. Even organizations that are leveraging orchestration or risk prioritization solutions are still left to handle an unmanageable amount of critical risks. However, the reality is that many risks can be traced back to a common root cause. This means a single fix can address many issues at once - that's a quick win. With the ability to automatically group risks based on root cause, security teams can prioritize fixes that address the highest number of risks with minimal changes, helping to clean the risk backlog and remain ahead of the curve.



Core Capability #2

Automated Root Cause Analysis

Understanding the root cause of cloud security risks is one of the most manual and complex parts of the remediation process. However, it's also one of the most critical. Implementing remediation strategies without fully understanding the root cause of the issue often results in the same risks resurfacing repeatedly. In fact, 80% of remediated risks today resurface shortly after remediation. By automating root cause analysis and tracing problems back to the specific lines of code that introduced them, security teams can implement more precise solutions and significantly reduce the likelihood of human error and recurring risks. Further, it allows security teams to save time on researching fixes and dedicate more time to implementing them.



Core Capability #3

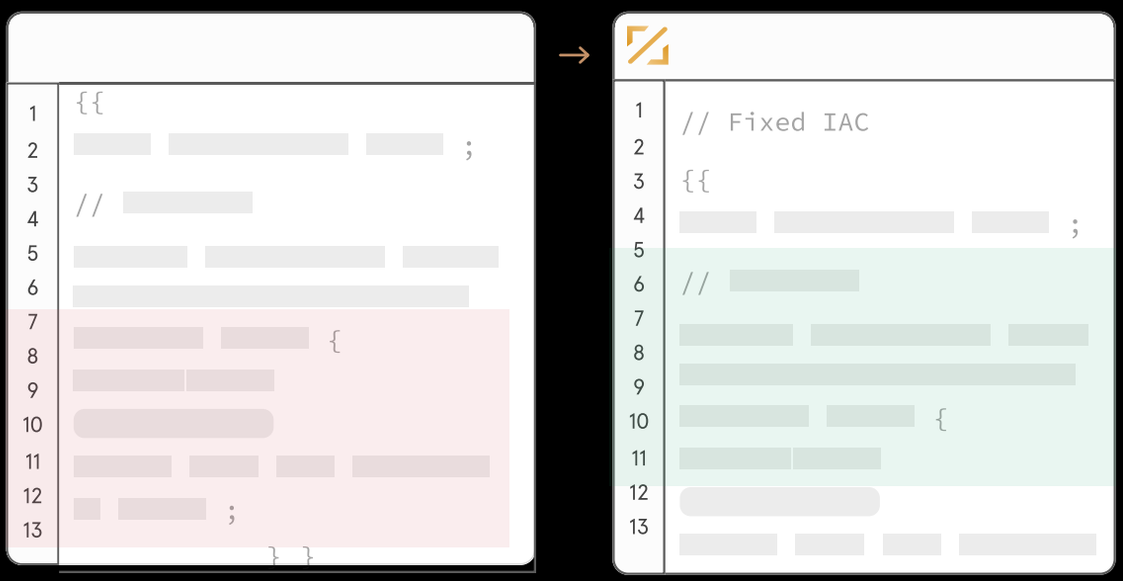
Artificial Intelligence (AI)

The recent advancements in AI have resulted in mass adoption and application - especially in the field of cybersecurity - to increase efficiency and reduce manual tasks and workload. In the case of risk remediation, AI can be applied to automatically craft the best resolution path for identified risks. Typically a process that requires weeks of back and forth meetings between security and DevOps is distilled down to a couple of clicks. Artificial Intelligence has the power to examine infinite options for resolution and provide the best possible path, while alleviating the burden of generating fixes and new code. Leveraging AI allows security teams to implement solutions faster than even and with greater precision.

Core Capability #4

Security as Code (SaC)

Proactively preventing risks is the dream of all security engineers. However, the manual nature of traditional risk remediation often leaves security teams in a reactive mode, without the ability to take a step back and ensure that the fixes implemented today can prevent future risks as well. The most effective way to do this is to take a code-based approach, leveraging the same systems that introduced the risk to remediate it. By using Infrastructure as Code (such as Terraform and CloudFormation), DevOps can quickly remediate issues at scale and as part of a safe deployment process, ensuring that fixes not only resolve immediate issues but also prevent future risks.



Core Capability #5

Mitigation Paths

In an ideal world, we would remediate everything. However, that's not always possible. There are many scenarios where remediation isn't an option - perhaps a patch isn't yet available, or the current infrastructure can't support an upgrade. In these cases, mitigation becomes crucial to reducing risk. While full remediation may take longer or can't be done, mitigation using existing controls and cloud-native services can be implemented immediately. For example, say you've identified a critical vulnerability in a public-facing cloud instance. Full remediation, which involves waiting for a patch and upgrading the vulnerable package, will take time. What if, in the meantime, you could mobilize mitigating controls? By leveraging existing security tools such as SASE, or by changing cloud configurations, you can reduce risk immediately.

Core Capability #6

Remediation Validation

Once a fix is implemented, security teams need to be able to quickly verify whether the issue has been fully resolved without going back to the team responsible for applying security remediations (e.g. DevOps). Being able to proactively verify that risks were actually remediated, enables security teams to follow the principle of "trust but verify". This can be achieved by using the power of open source, leaning on the security community. Whether you are using enterprise security tools or best-of-breed open source tools for risk identification and scanning capabilities, security teams should be able to quickly validate that risks have been remediated as part of CI/CD to close the remediation loop and confidently move on to the next problem.

It's Time We Evolve

Traditional vulnerability and risk management has failed us. While security teams are spending endless hours researching and implementing fixes, they struggle to make a real impact on risk reduction. Current approaches has resulted in high security tax and security debt - where the lack of automation and innovation is impacting overall efficiency and creating an accumulation of unresolved security issues that represent long-term risk.

Attackers are evolving and exploiting vulnerabilities faster than ever, which highlights the urgent need for security teams to adopt new technologies and approaches to keep up. Organizations should consider adopting these six core capabilities to shift from traditional risk remediation to risk resolution.

About ZEST Security

ZEST offers an AI-powered risk resolution platform that redefines cloud risk remediation for security and DevOps teams. ZEST resolution paths provide both mitigation and remediation 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 Hanaco Ventures, Silvertech Ventures and angel investors, ZEST has offices in New York City and Tel Aviv. For more information visit www.zestsecurity.io

ZEST