aidoc CASE STUDY

> Ermetic goes beyond permissions visibility to reveal IAM risk context that informs our busy devops team, facilitating their efforts in mitigating risk and minimizing disruption.
>
> Guy Reiner, co-founder and VP of R&D at Aidoc

Aidoc is the leading provider of artificial intelligence solutions that support and enhance the impact of radiologist diagnostic power. The company's solutions aid radiologists in reducing turnaround time and increasing quality and efficiency by flagging acute anomalies in real time.

The Challenge

Founded in early 2016, Aidoc offers an AI medical diagnostics SaaS platform that is "always on." The solution and its development run on AWS. The devops team handles the organization's cloud security. The team knew that its IAM permissions configurations were potentially an ongoing security threat due to the complexity and opaqueness of public cloud environments. With many things on their plate, the devops team was always looking for time saving ways to better monitor and remediate access risk, including by right-sizing policies.

The Solution

Upon reviewing Ermetic, Guy Reiner, co-founder and VP of R&D at Aidoc, was enthused. After a simple set up, he saw Ermetic rapidly detect multiple excessive permissions and inactive roles in the Aidoc cloud infrastructure -- and knew these to be fertile ground for threat actors. The Ermetic proof of concept also showed how such potential risks could be easily remediated, and how the entitlements management platform could help Aidoc govern third party access and privileged identities, and trace any access flaws or resource vulnerabilities to their root cause.

At first concerned about bringing Ermetic to his team's attention so as not to burden them "with one more management tool," Guy eventually chose to let them do their own due diligence. The Aidoc devops team quickly found the Ermetic platform made many of their IAM risk management tasks easier and, in presenting a visual mapping of all their cloud identities and permissions, proved considerably more informative than the AWS console. Ultimately, the team drove Aidoc's decision to adopt Ermetic.

> We're next setting our sights on implementing the least privilege policies that Ermetic generates from actual use -- that kind of automation is right up there with devops best practice by enabling us to remediate at scale and shift left to harden net-needed access into our infrastructure.
>
> Guy Reiner, co-founder and VP of R&D at Aidoc

Digging deeper, the devops team found they could effectively use the Ermetic platform, via its Findings view, as an actionable roadmap for prioritizing their IAM and other configuration risks. The view delineates risks by criticality and scope, helping Aidoc decide which risks to tackle first and which to address progressively over time to proactively reduce their attack surface.

Said Reiner, "Ermetic goes beyond permissions visibility to reveal IAM risk context that informs our busy devops team, facilitating their efforts in mitigating risk and minimizing disruption. We're next setting our sights on implementing the least privilege policies that Ermetic generates from actual use -- that kind of automation is right up there with devops best practice by enabling us to remediate at scale and shift left to harden net-needed access into our infrastructure."

About Ermetic

Ermetic is an award-winning public cloud security platform that enables enterprises to govern all identities and access privileges, remediate risk swiftly and enforce least privilege at scale. Through continuous analysis, Ermetic generates least-privilege access policies based on actual use. It is the first solution to provide full-stack insight into the effectiveness and risks of access entitlements granted by configuration of identities, compute resources, data stores and the network.

For more information, visit https://ermetic.com/