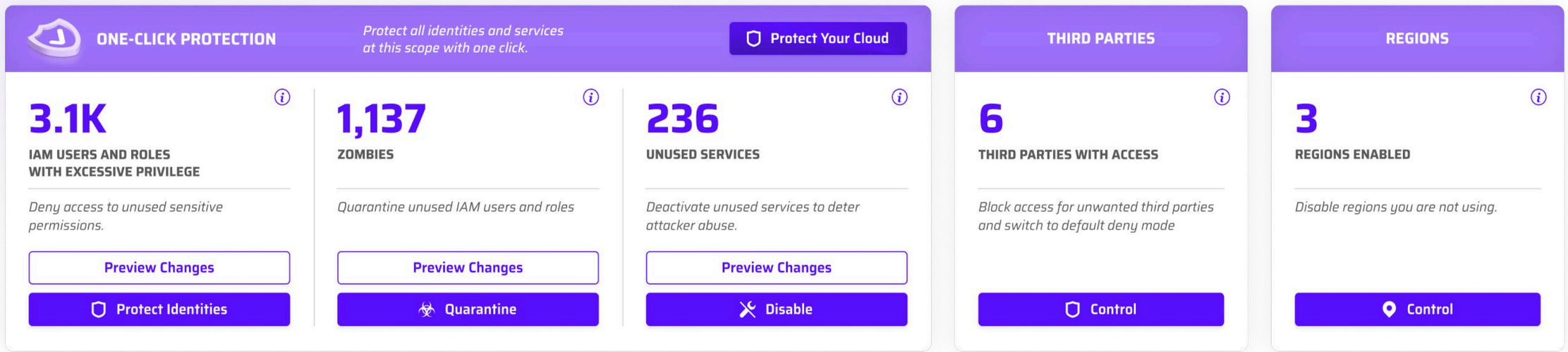
What Does The Cloud Permissions Firewall Protect?



Excessive Privileged Permissions

Excessive privileged permissions refer to the ~3,500 most privileged cloud permissions granted to identities (both human and machine) that exceed the minimum necessary to perform their tasks and therefore, are going unused. Excessive access to privileged permissions increases your attack surface by creating more opportunities for malicious actors to misuse cloud permissions for unauthorized access, data theft, and business disruption.

How we help: Cloud Permissions Firewall monitors privileged permissions usage to generate a centralized policy that restricts privileged permissions from identities not using them. Identities who need access are added as exemptions to the policy to ensure zero disruption to development. Default-deny is enforced automatically for new identities and new access is granted seamlessly with a permissions-on-demand automated workflow.

Zombie (Unused) Identities

Zombies (Unused identities) are dormant users or roles, such as old employee accounts, outdated service accounts, and unused APIs, that are no longer actively used (quiet for over 90 days) but still exist within the cloud environment. They often remain unnoticed, making them prime targets for malicious activities.

How we help: Cloud Permissions Firewall identifies zombie identities and then quarantines the identity from use. This means all permissions are stripped from the identity, rendering it useless for an attacker. This secures unused identities without the fear or risk of deleting them or the operational burden. You can ‘wake up’ zombies from their quarantine with the automated permissions-on-demand workflow.

Unused Services

Unused services are cloud services that are not actively used but are still accessible within the cloud environment. Unused services offer opportunities for attackers to disrupt your environment, increase operational costs and fly under the radar.

How we help: Cloud Permissions Firewall offers an easy way to disable unused services according to the scope of your choosing. You can disable services in one account or environment, while allowing access in another. This ease of protection alleviates the operational burden of policy management.

Unused Regions

Unused regions are geographical regions within a cloud provider's infrastructure that are not actively used for deploying services or storing data. Unused regions can be exploited by insiders or attackers to deploy unmonitored resources, potentially bypassing security controls. They also pose risks related to data sovereignty and compliance, as data might inadvertently be stored in unauthorized regions.

How we help: With a simple toggle on and off button, you can instantly protect unused regions from any deployments, service usage or permissions activity.

Third-Party Access

Third-party access is often required by external entities like vendors or applications, but it is one of the leading causes of cloud security breaches. Without proper controls, these external entities can expose sensitive data, increase your attack surface, and create compliance risks.

How we help: Cloud Permissions Firewall automatically identifies and blocks unauthorized third-party access while enforcing a default-deny policy to prevent future risks. Approvals and updates are handled quickly through automated workflows, making it simple to keep third-party access secure and centrally managed.

Just in Time Access

Eliminating standing privileges is a best practice to reduce your attack surface, particularly for human users in production accounts. Implementing it in the cloud often requires a new external identity layer with additional infrastructure that creates a new workstream and new products to learn.

How we help: By building a JIT solution using the native cloud IAM infrastructure, Sonrai gets you to zero standing privilege without introducing new bastion hosts, jump boxes, or user interfaces. All requests and approvals can be handled in existing ChatOps (like Slack, Teams, or email). Smart AI log processing gives you session summaries fast and without manual work.

Start using the Cloud Permissions Firewall today

ONBOARD YOUR CLOUD IN	GET CONTROL OF PERMISSIONS IN	EXPLORE THE FULL PRODUCT FOR
15 MINUTES	**2** HOURS	**14** DAYS

sonrai.co/trial