ermetic

Whitepaper

Why managing cloud entitlements is nearly impossible… and how to do it

Ermetic for CIEM

Managing cloud entitlements and least privilege with success

To reduce their cloud attack surface, organizations need deep insight into identities, entitlements and misconfigurations -- and the ability to auto-mitigate risk

Executive Summary

Your job has likely gotten more intense lately. Whether it's due to the anomaly of 2020-2021 or your organization's digital momentum, you are part of a huge trend: public cloud use is growing at a staggering pace each year, with the Infrastructure as a Service segment growing the fastest. Amid that growth, cause for concern:

75% of cloud security failures will result from mismanagement of IAM privileges by 2023

[Source: Gartner]

With traditional perimeters gone, identities are now the largest cloud infrastructure attack surface. Recent breaches show that attackers are exploiting mismanaged IAM privileges to penetrate an organization's cloud infrastructure to reach sensitive data. To strengthen your cloud infrastructure against such risks, you need full visibility into the identities with access to your cloud resources as well as an understanding of any associated risk and the means to mitigate quickly.

Do you have the capabilities for securing, managing and investigating your cloud entitlements effectively? If not, you're not alone. A recent IDC survey sponsored by Ermetic found that 98% of respondents had at least one cloud breach in the last 18 months – and 83% said at least one was access related.

Ermetic is a comprehensive security platform for AWS, Azure and GCP for effective cloud infrastructure entitlement management (CIEM) and cloud security posture management (CSPM). The platform provides visibility into all identities across the full-stack lifecycle to accurately detect, measure and mitigate risk to resources. Its unique identity first approach makes it the strongest CIEM solution available, bringing to light the toxic and often hidden scenarios of identity, network and resource configuration that put your data at risk.

Using Ermetic can help you:

- Visualize all entitlements, resources and access relationships, and related risks, across multicloud environments
- Govern risk and manage access by privileged identities and third parties
- Eliminate excessive entitlements for human and machine identities
- Review and certify entitlements (across admins, developers and DevOps, as well as human and SaaS third parties)
- Detect and monitor public exposure and shared resources
- Generate least-privilege policies and automate remediation
- Investigate access activities and anomalies
- Automate just-enough and just-in-time permissions for privileged access

Ermetic also provides robust capabilities for managing your cloud security posture, including:

- Manage your cloud asset inventory
- Detect misconfigurations
- Monitor and report on compliance with industry standards and practices

It's a responsibility, and privilege, to be vested with protecting what is likely your organization's biggest growth platform. This paper explores how to get a grip on the weakest link in securing your cloud infrastructure -- identities -- and govern them at scale with minimal effort.

The challenge - A sad state of affairs

Recent major breaches show that identities play a role in virtually every attack scenario in cloud infrastructure. Let's look at why:

- Excessive entitlements. In the interest of speed, organizations tend to over privilege identities when spinning up cloud environments
- Shift left is moving infrastructure security to teams with other priorities. DevOps teams have lots on their plate; security is not usually their top priority.
- Driving blind. Tracking entitlements and their use is hard. Cloud provider tools lack the visibility or context to give a full picture of access to resources and remediate access risk at scale and across clouds.
- Legacy PAM and IGA are limited by their on-prem DNA. In cloud infrastructure they lack granular service or resource level visibility, and cannot identify or remediate entitlement risks and excessive permissions.

Securing cloud infrastructure calls for a deep, unified view into all identities and cloud resources to understand the full stack of access entitlements and privileges, and associated risk. You must be able to secure all privileged identities and minimize their risk of being compromised. You need the means for removing excessive and risky privileges, managing access control and permissions, investigating activities and behavior, and applying least privilege across the board, throughout the cloud identity lifecycle.

There's urgency. The longer you wait to understand and undo identity risk, the greater the complexity in doing so as the number of privileged identities, exposure risks, excessive permissions and sensitive resources in your environment continue to grow.

The solution - Securing cloud infrastructure identity-first

The leading analyst groups defined several security categories that address the high importance of managing entitlements and access policy throughout the identity lifecycle. These solutions -- Cloud Infrastructure Entitlement Management – CIEM (Gartner), Cloud Native Application Protection Platforms – CNAPP (Gartner) and Cloud Infrastructure Governance – CIG (Forrester) – are expected to keep pace with evolving protection requirements for cloud-native applications, spanning virtual machines, containers and serverless workloads.

Ermetic is the first identity-first solution to offer full-stack lifecycle management of the entitlements granted by configuration of identities, compute resources, data stores and the network.

Ermetic helps security, devops and IAM practitioners:

- Gain a full, contextual view into human and machine identities to identify privileged identities and evaluate all permission configurations to understand risky or excessive privileges, and how associated compute, data and network resources map across their organization's multi cloud environment
- Leverage advanced analyses and machine-learning algorithms to address critical cloud security issues and identify identity and configuration risks and threats
- Mitigate and prevent risks at scale using automatically generated least privilege policies that integrate seamlessly with ticketing, CI/CD pipelines and IaC

How does it deploy? An agentless, API-based SaaS solution, Ermetic requires nothing to deploy and just minutes to set up. It supports the leading cloud service providers and offers deep interoperability with cloud-based identity providers. Ermetic starts aggregating data in minutes after deployment, bringing actionable information into view almost instantly.

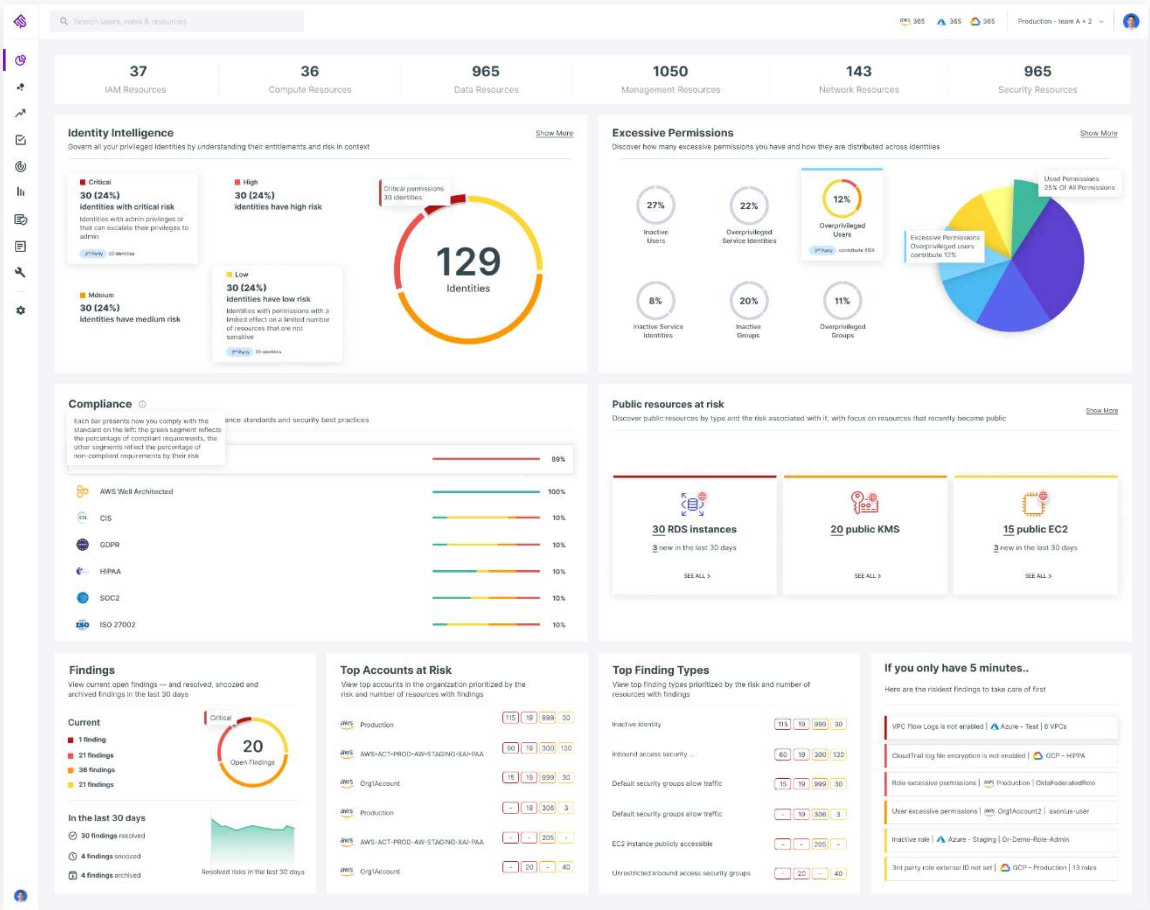
Who can use it? No prerequisites are required. Ermetic meets the needs of cloud customers of all sizes, from large enterprises to smaller, cloud-native organizations. In cloud environments, all organizations have the same IAM challenges.

How do I use it? Ermetic gives organizations control over their cloud infrastructure that they were unable to achieve before. Ermetic empowers security, devops and IAM teams – even with little cloud security expertise -- to see deeply into the full cloud assets inventory and permissions relationships, govern privileged entities, detect misconfigurations and practice least privilege in modern multi-cloud environments.

Key use cases: How you can apply Ermetic

Visualize all cloud assets and relationships

The Ermetic management dashboard provides a visual overview, with click-through deep dive, into all identities in your environment and any risk caused by excessive permissions, misconfigurations, internet exposure, compliance issues and anomalies. The one-stop view helps answer: What are my top IAM risks? How many entitlements are excessive and what is the potential impact? Where are we falling short on compliance? Which identities are privileged and can be compromised? How much is my environment exposed to the outside?



Identity Intelligence

Govern all your privileged identities by understanding their entitlements and risk in context

Critical: 30 (24%) identities with critical risk. Identities with admin privileges or that can escalate their privileges to admin

High: 30 (24%) identities have high risk

Mdeium: 30 (24%) identities have medium risk

Low: 30 (24%) identities have low risk. Identities with permissions with a limited effect on a limited number of resources that are not sensitive

Excessive Permissions

Discover how many excessive permissions you have and how they are distributed across identtiies

Compliance

Each bar presents how you comply with the standard on the left: the green segment reflects the percentage of compliant requirements, the other segments reflect the percentage of non-compliant requirements by their risk

ance standards and security best practices

Public resources at risk

Discover public resources by type and the risk associated with it, with focus on resources that recently became public

Findings

View current open findings — and resolved, snoozed and archived findings in the last 30 days

Current
- 1 finding
- 21 findings
- 36 findings
- 21 findings

In the last 30 days
- 30 findings resolved
- 4 findings snoozed
- 4 findings archived

Top Accounts at Risk

View top accounts in the organization prioritized by the risk and number of resources with findings

aws Production	115	19	999	30
aws AWS-ACT-PROD-AW-STAGING-XAI-PAA	60	19	300	130
aws Org1Account	15	19	999	30
aws Production	-	19	306	3
aws AWS-ACT-PROD-AW-STAGING-XAI-PAA	-	-	205	-
aws Org1Account	-	20	-	40

Top Finding Types

View top finding types prioritized by the risk and number of resources with findings

Inactive identity	115	19	999	30
Inbound access security ...	60	19	300	130
Default security groups allow traffic	15	19	999	30
Default security groups allow traffic	-	19	306	3
EC2 instance publicly accessible	-	-	205	-
Unrestricted inbound access security groups	-	20	-	40

If you only have 5 minutes..

Here are the riskiest findings to take care of first

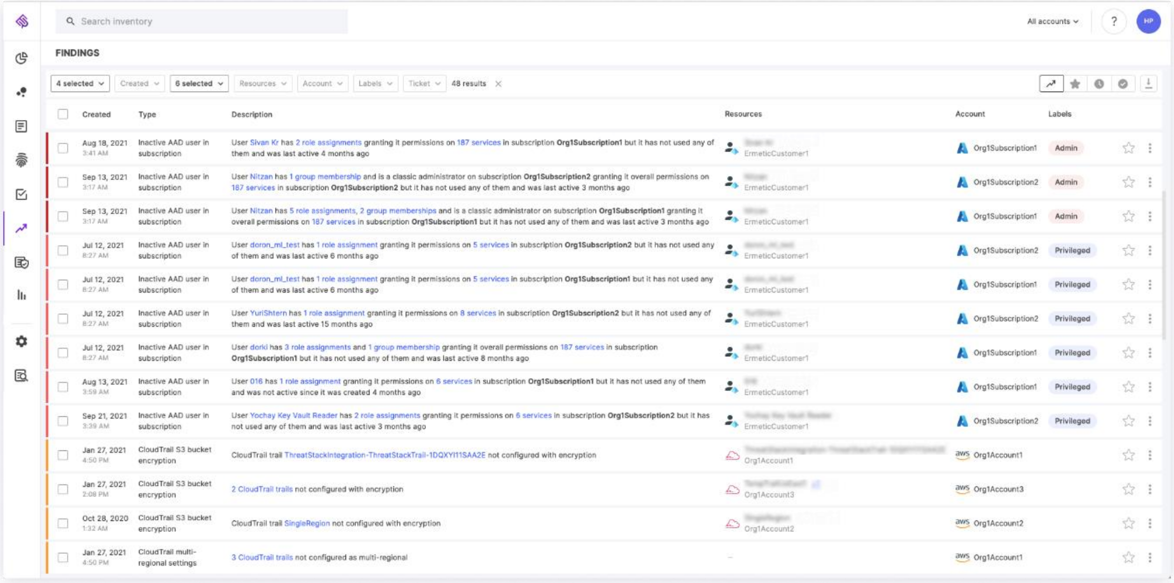
- VPC Flow Logs is not enabled | Azure - Test | 6 VPCs
- CloudTrail log file encryption is not enabled | GCP - HIPPA
- Role excessive permissions | aws Production | OktaFederatedRole
- User excessive permissions | aws Org1Account2 | axonius-user
- Inactive role | Azure - Staging | Or-Demo-Role-Admin
- 3rd party role external ID not set | GCP - Production | 13 roles

Ermetic management dashboard: Get an overview of all entitlement risks, exposed resources and misconfigurations in your cross-cloud infrastructure

Prioritize and remediate risk

Ermetic provides a prioritized view into the entitlement risks in your cloud environment. It shows over-permissive identities by category, including inactive and overprivileged users, inactive and overprivileged service identities, and overprivileged groups. Start your day by reviewing one by one the access and configuration risks that Ermetic has detected, honing in by level of severity. Mitigate risk by following easy and clear remediation steps for removing excessive permissions and applying policy changes that, for example, minimize exposure to sensitive resources, remove dangerous privileges and eliminate inactive users. Ermetic works with your tech stack, including Datadog, Slack, Splunk, and email, ServiceNow and Jira, and Okta and Azure Active Directory, to seamlessly communicate on risk and deliver new least privilege policies in your IT and DevOps workflows.

Actionable views help you drill down to answer: Is the severity of the risk warranted? Has the entitlement ever been used? Can the user self-escalate to an admin role, creating unwarranted risk?



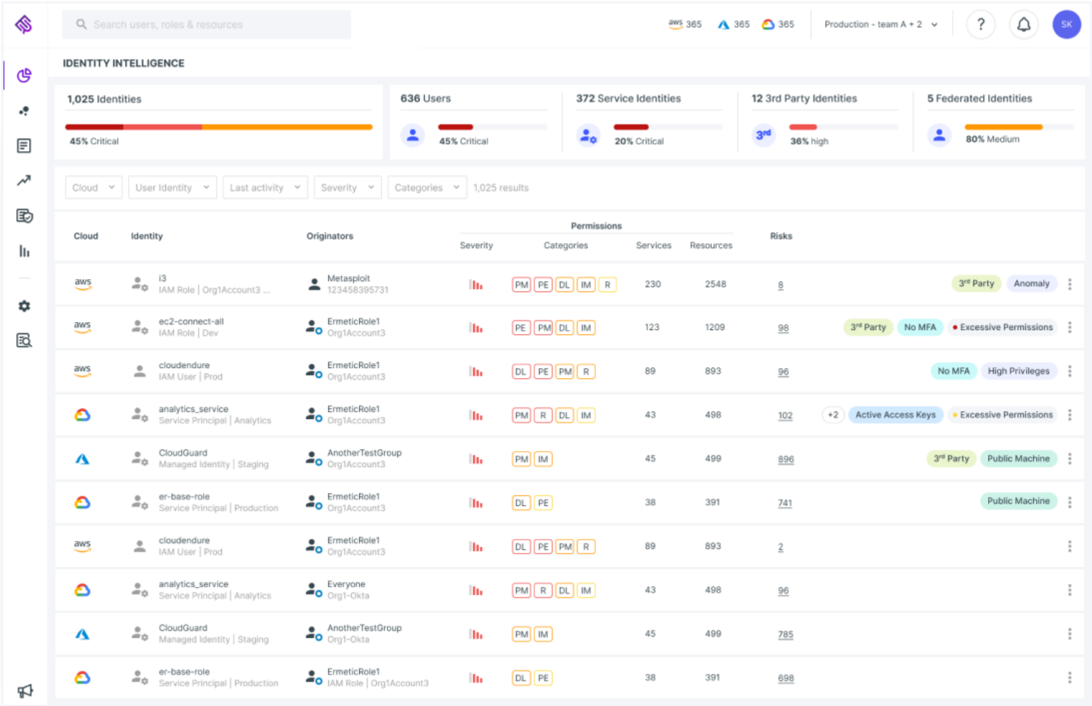
☐	Created	Type	Description	Resources	Account	Labels
☐	Aug 18, 2021 3:41 AM	Inactive AAD user in subscription	User Sivan Kr has 2 role assignments granting it permissions on 187 services in subscription **Org1Subscription1** but it has not used any of them and was last active 4 months ago	[redacted] ErmeticCustomer1	Org1Subscription1	Admin
☐	Sep 13, 2021 3:17 AM	Inactive AAD user in subscription	User Nitzan has 1 group membership and is a classic administrator on subscription **Org1Subscription2** granting it overall permissions on 187 services in subscription **Org1Subscription2** but it has not used any of them and was last active 3 months ago	[redacted] ErmeticCustomer1	Org1Subscription2	Admin
☐	Sep 13, 2021 3:17 AM	Inactive AAD user in subscription	User Nitzan has 5 role assignments, 2 group memberships and is a classic administrator on subscription **Org1Subscription1** granting it overall permissions on 187 services in subscription **Org1Subscription1** but it has not used any of them and was last active 3 months ago	[redacted] ErmeticCustomer1	Org1Subscription1	Admin
☐	Jul 12, 2021 8:27 AM	Inactive AAD user in subscription	User doron_ml_test has 1 role assignment granting it permissions on 5 services in subscription **Org1Subscription2** but it has not used any of them and was last active 6 months ago	[redacted] ErmeticCustomer1	Org1Subscription2	Privileged
☐	Jul 12, 2021 8:27 AM	Inactive AAD user in subscription	User doron_ml_test has 1 role assignment granting it permissions on 5 services in subscription **Org1Subscription1** but it has not used any of them and was last active 6 months ago	[redacted] ErmeticCustomer1	Org1Subscription1	Privileged
☐	Jul 12, 2021 8:27 AM	Inactive AAD user in subscription	User YuriShtern has 1 role assignment granting it permissions on 8 services in subscription **Org1Subscription2** but it has not used any of them and was last active 15 months ago	[redacted] ErmeticCustomer1	Org1Subscription2	Privileged
☐	Jul 12, 2021 8:27 AM	Inactive AAD user in subscription	User dorki has 3 role assignments and 1 group membership granting it overall permissions on 187 services in subscription **Org1Subscription1** but it has not used any of them and was last active 8 months ago	[redacted] ErmeticCustomer1	Org1Subscription1	Privileged
☐	Aug 13, 2021 3:59 AM	Inactive AAD user in subscription	User 016 has 1 role assignment granting it permissions on 6 services in subscription **Org1Subscription1** but it has not used any of them and was not active since it was created 4 months ago	[redacted] ErmeticCustomer1	Org1Subscription1	Privileged
☐	Sep 21, 2021 3:39 AM	Inactive AAD user in subscription	User Yochay Key Vault Reader has 2 role assignments granting it permissions on 6 services in subscription **Org1Subscription2** but it has not used any of them and was last active 3 months ago	[redacted] ErmeticCustomer1	Org1Subscription2	Privileged
☐	Jan 27, 2021 4:50 PM	CloudTrail S3 bucket encryption	CloudTrail trail ThreatStackIntegration-ThreatStackTrail-1DQXYI11SAA2E not configured with encryption	[redacted] Org1Account1	aws Org1Account1	
☐	Jan 27, 2021 2:08 PM	CloudTrail S3 bucket encryption	2 CloudTrail trails not configured with encryption	[redacted] Org1Account3	aws Org1Account3	
☐	Oct 28, 2020 1:32 AM	CloudTrail S3 bucket encryption	CloudTrail trail SingleRegion not configured with encryption	[redacted] Org1Account2	aws Org1Account2	
☐	Jan 27, 2021 4:50 PM	CloudTrail multi-regional settings	3 CloudTrail trails not configured as multi-regional	–	aws Org1Account1	

Findings view: Start your day assessing and remediating the greatest permissions risks, reducing your organization’s attack surface

Govern privileged identities

Ermetic reveals all privileged identities in your cloud infrastructure by type, including user, service, third party applications and federated identities from identity providers. It enables you to understand what a privileged identity is entitled to do, including its ability to manage permissions, leak data, modify infrastructure, escalate privilege and/or carry out reconnaissance -- helping you assess if the identity is overprivileged.

Ermetic also gives details about an identity's risk factors, such as use of access keys and multi-factor authentication, and exposure of data to the internet or third parties. Ermetic enables you to govern privileged identities with efficiency and ease by monitoring them, eliminating their excessive entitlements and acting on an ongoing basis to minimize their risk of being compromised by an external -- or internal -- threat actor.



IDENTITY INTELLIGENCE

1,025 Identities — 45% Critical

636 Users — 45% Critical

372 Service Identities — 20% Critical

12 3rd Party Identities — 36% high

5 Federated Identities — 80% Medium

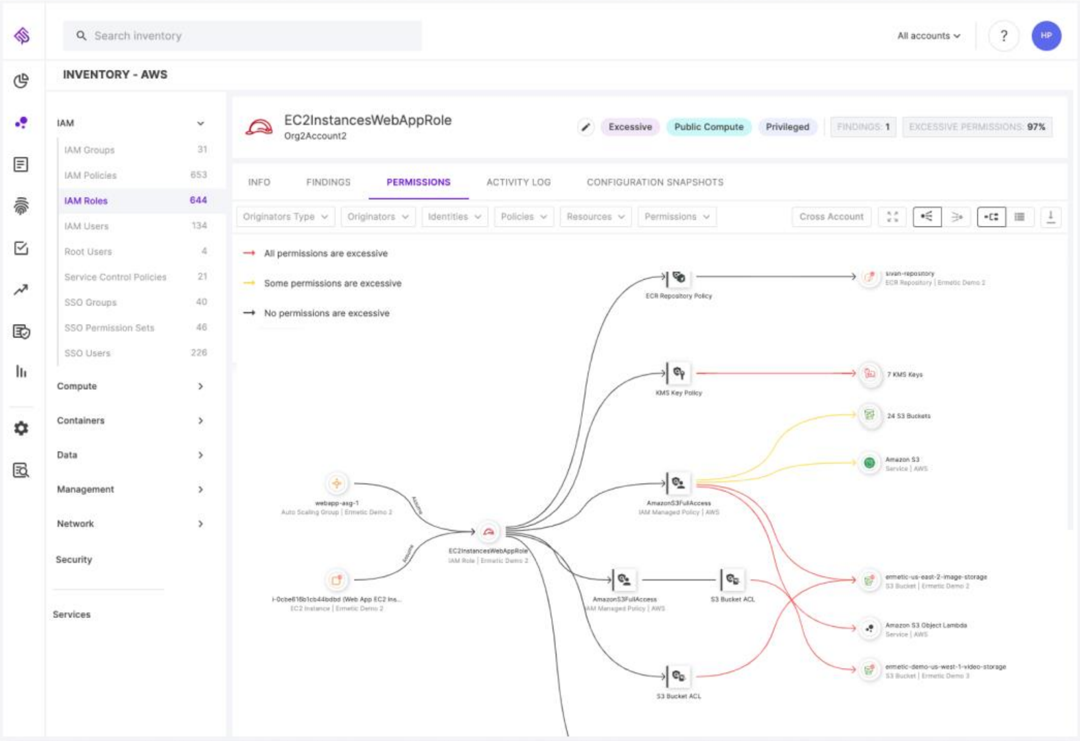
Cloud · User Identity · Last activity · Severity · Categories · 1,025 results

Cloud	Identity	Originators	Permissions				Risks	
			Severity	Categories	Services	Resources		
aws	i3 IAM Role | Org1Account3 ...	Metasploit 123458395731	▮	PM PE DL IM R	230	2548	8	3rd Party · Anomaly
aws	ec2-connect-all IAM Role | Dev	ErmeticRole1 Org1Account3	▮	PE PM DL IM	123	1209	98	3rd Party · No MFA · ● Excessive Permissions
aws	cloudendure IAM User | Prod	ErmeticRole1 Org1Account3	▮	DL PE PM R	89	893	96	No MFA · High Privileges
☁	analytics_service Service Principal | Analytics	ErmeticRole1 Org1Account3	▮	PM R DL IM	43	498	102	+2 · Active Access Keys · ● Excessive Permissions
▲	CloudGuard Managed Identity | Staging	AnotherTestGroup Org1Account3	▮	PM IM	45	499	896	3rd Party · Public Machine
☁	er-base-role Service Principal | Production	ErmeticRole1 Org1Account3	▮	DL PE	38	391	741	Public Machine
aws	cloudendure IAM User | Prod	ErmeticRole1 Org1Account3	▮	DL PE PM R	89	893	2	
☁	analytics_service Service Principal | Analytics	Everyone Org1-Okta	▮	PM R DL IM	43	498	96	
▲	CloudGuard Managed Identity | Staging	AnotherTestGroup Org1-Okta	▮	PM IM	45	499	785	
☁	er-base-role Service Principal | Production	ErmeticRole1 IAM Role | Org1Account3	▮	DL PE	38	391	698	

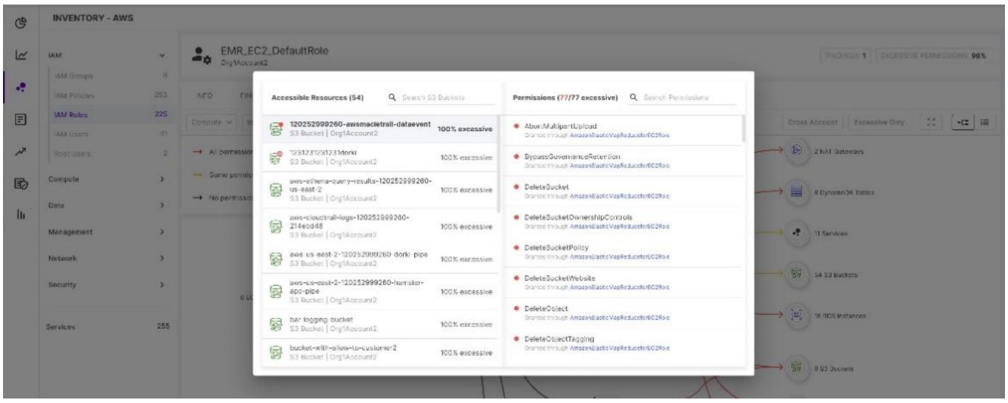
Identity intelligence view: Govern all privileged identities in your cloud infrastructure aided by deep and contextual insight into entitlements and risk

Review and certify entitlements

Ermetic lets you deep dive into entitlements of specific entities, such as IAM role, user or group to determine if the assigned access is justified and to mitigate as needed. Ermetic shows the entitlements for every identity at the most granular level of a specific resource or permission -- far beyond the capabilities available in cloud-native tools like AWS Access Advisor or Azure RBAC. Ermetic presents not just the general information for a specific entity but also a visual graph showing all the entity's permissions, color-coded for easy understanding of the extent to which permissions are excessive. You can assess the information and, importantly, review Ermetic's findings of unnecessary or dangerous access, and execute recommended remediation steps at a click.



View entitlements by role and user, guided by color coding that shows excessive permissions by severity, filter for more detail, remediate at a click



Accessible Resources (54)

120252999260-awsmacietrail-dataevent
S3 Bucket | Org1Account2 — 100% excessive

123123123123dorki
S3 Bucket | Org1Account2 — 100% excessive

aws-athena-query-results-120252999260-us-east-2
S3 Bucket | Org1Account2 — 100% excessive

aws-cloudtrail-logs-120252999260-214e0d48
S3 Bucket | Org1Account2 — 100% excessive

aws-us-east-2-120252999260-dorki-pipe
S3 Bucket | Org1Account2 — 100% excessive

aws-us-east-2-120252999260-hamster-apc-pipe
S3 Bucket | Org1Account2 — 100% excessive

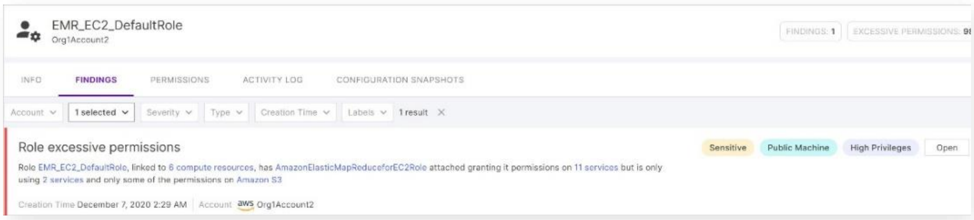
bar logging bucket
S3 Bucket | Org1Account2 — 100% excessive

bucket-with-allow-to-customer2
S3 Bucket | Org1Account2 — 100% excessive

Permissions (77/77 excessive)

- AbortMultipartUpload
  Granted through AmazonElasticMapReduceforEC2Role
- BypassGovernanceRetention
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteBucket
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteBucketOwnershipControls
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteBucketPolicy
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteBucketWebsite
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteObject
  Granted through AmazonElasticMapReduceforEC2Role
- DeleteObjectTagging
  Granted through AmazonElasticMapReduceforEC2Role

See detailed entitlement information in list format; click on an item to drill down

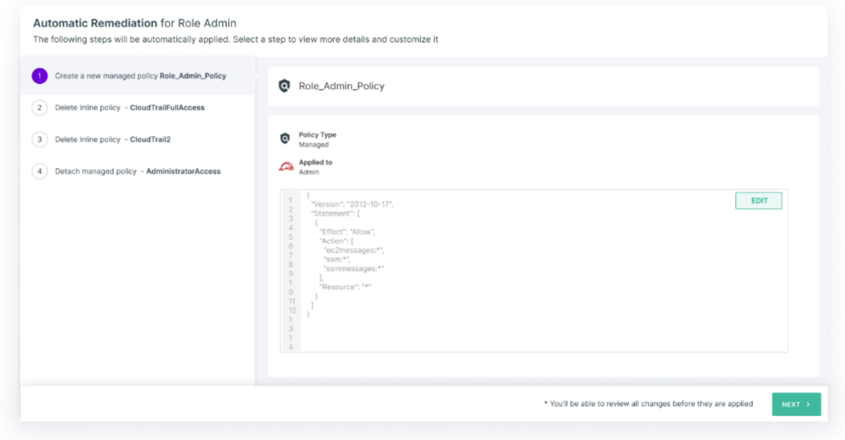


Role excessive permissions

Role EMR_EC2_DefaultRole, linked to 6 compute resources, has AmazonElasticMapReduceforEC2Role attached granting it permissions on 11 services but is only using 2 services and only some of the permissions on Amazon S3

Creation Time December 7, 2020 2:29 AM | Account aws Org1Account2

Review any role to understand why Ermetic has defined an entitlement as risky or excessive



Automatic Remediation for Role Admin

The following steps will be automatically applied. Select a step to view more details and customize it

1. Create a new managed policy **Role_Admin_Policy**
2. Delete inline policy - **CloudTrailFullAccess**
3. Delete inline policy - **CloudTrail2**
4. Detach managed policy - **AdministratorAccess**

Role_Admin_Policy

Policy Type
Managed

Applied to
Admin

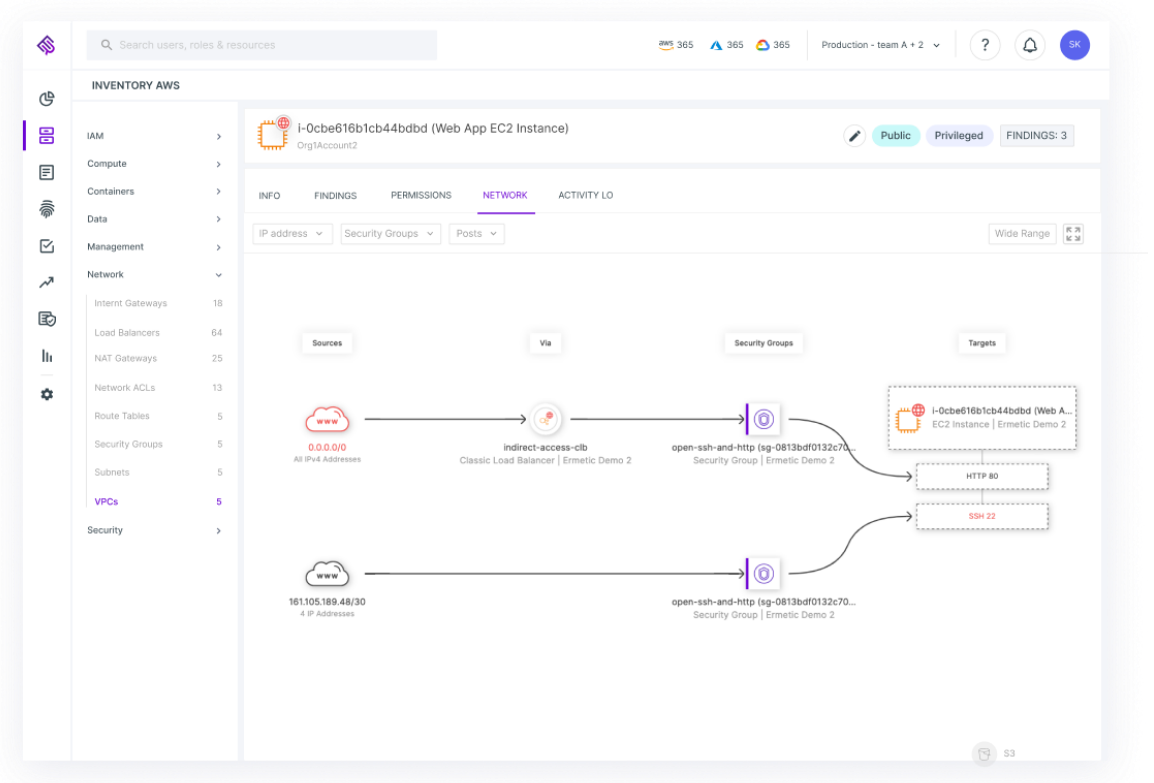
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2messages:*",
        "ssm:*",
        "ssmmessages:*"
      ],
      "Resource": "*"
    }
  ]
}
```

* You'll be able to review all changes before they are applied

Follow easy steps for remediation

Detect and mitigate access to sensitive resources

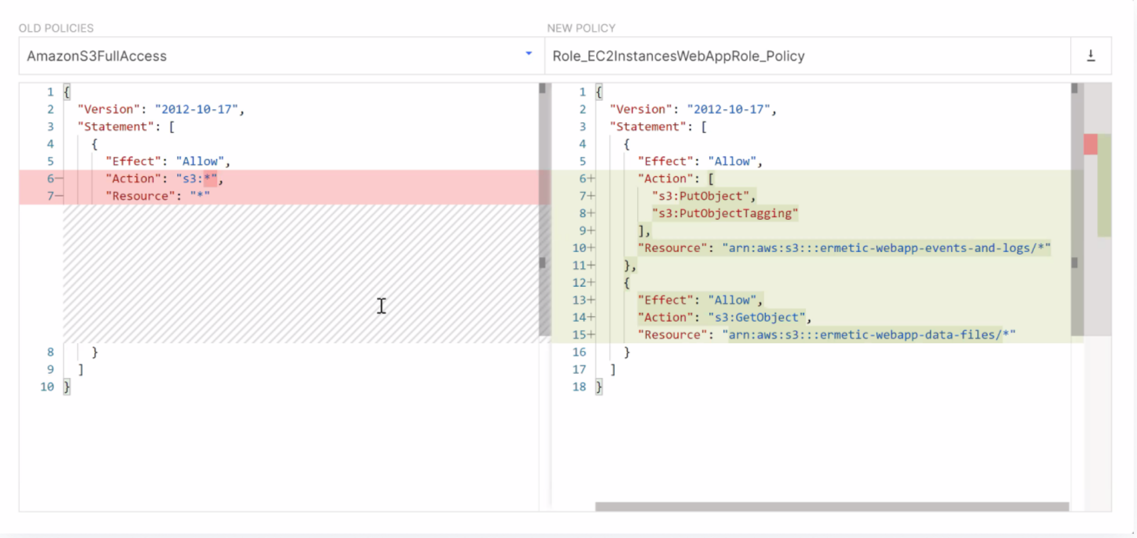
Ermetic enables you to flag a resource -- data, compute, security or management –as sensitive, and filter views to see which users and roles can access it, and if their permissions are excessive. It cuts through complexity to reveal network access and publicly exposed resources. It takes a multi-vectored approach to give a true assessment of risk. For example, Ermetic detects if entitlements expose a database, yet the risk is low due to adequate network configuration protection. You can assess the information and remediate at a click, updating the policy to minimize the potential risk.



Detect and monitor risk in the context of a resource exposed to the internet and the security validity of its entitlements

Apply least privilege policies and automate remediation

Ermetic analyzes data from cloud activity logs such as AWS CloudTrail to generate resource-level, least-privilege policy based on actual usage. Ermetic auto-remediates risky privileges and faulty configurations directly with wizards. You can also use Ermetic to enforce least privilege policies across multicloud environments. Ermetic enables you to ticket auto-generated, optimized policies and configuration fixes within your CI/CD pipelines (Jira, ServiceNow…) and generate IaC snippets in Terraform and CloudFormation, accelerating your shift-left efforts.



OLD POLICIES: AmazonS3FullAccess

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

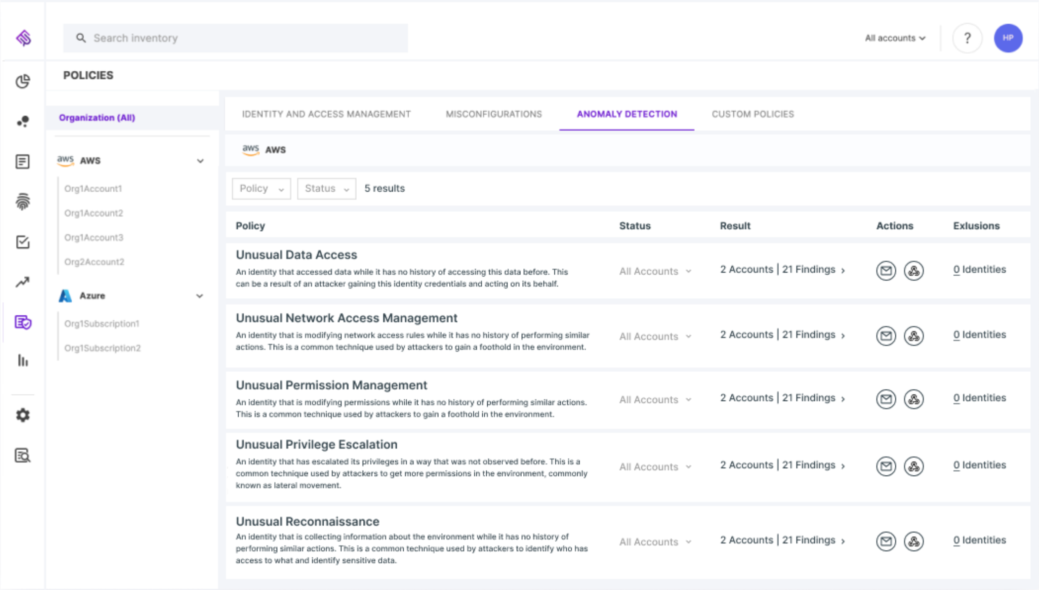
NEW POLICY: Role_EC2InstancesWebAppRole_Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:::ermetic-webapp-events-and-logs/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::ermetic-webapp-data-files/*"
    }
  ]
}
```

Remediate risky and excessive permissions with the automatically generated least-privilege access policy

Monitor and investigate anomalies and threats

Ermetic helps improve your cloud security posture by detecting anomalies through continuous risk analysis against behavioral baselines. It enables easy viewing of enriched access logs. Ermetic also detects identity-based threats, including unusual data access, privilege escalation and unexpected changes to permissions. It spots changes in login and audit settings – and to network configuration. Ermetic picks up on unusual reconnaissance and use of access keys across your public cloud environment. You can conduct smart searches by identity, entitlement or resource.

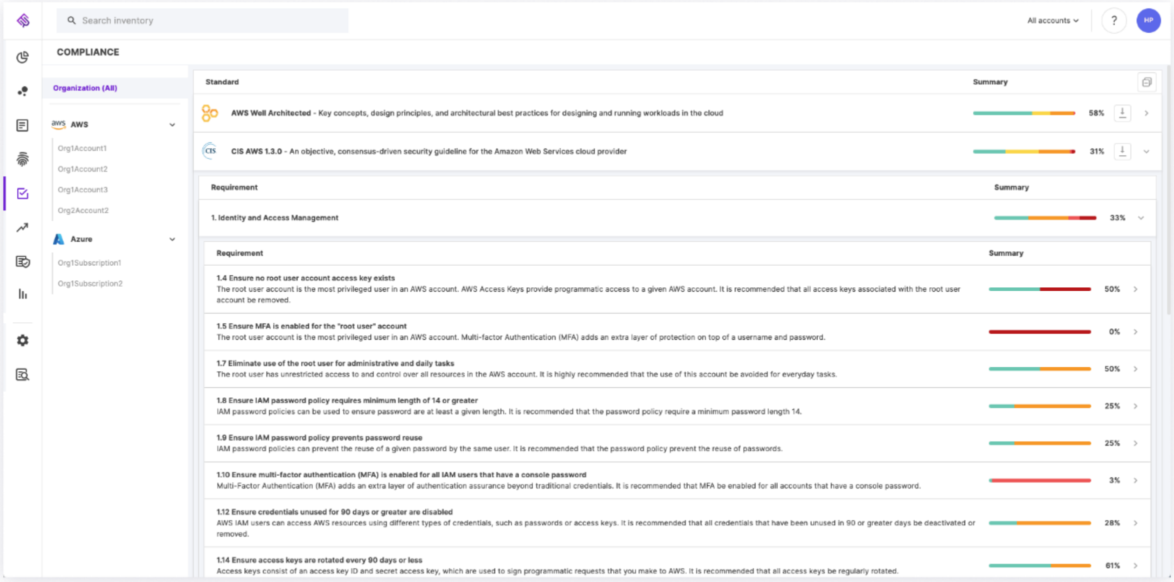


Policy	Status	Result	Actions	Exlusions
Unusual Data Access An identity that accessed data while it has no history of accessing this data before. This can be a result of an attacker gaining this identity credentials and acting on its behalf.	All Accounts	2 Accounts | 21 Findings ›	✉	0 Identities
Unusual Network Access Management An identity that is modifying network access rules while it has no history of performing similar actions. This is a common technique used by attackers to gain a foothold in the environment.	All Accounts	2 Accounts | 21 Findings ›	✉	0 Identities
Unusual Permission Management An identity that is modifying permissions while it has no history of performing similar actions. This is a common technique used by attackers to gain a foothold in the environment.	All Accounts	2 Accounts | 21 Findings ›	✉	0 Identities
Unusual Privilege Escalation An identity that has escalated its privileges in a way that was not observed before. This is a common technique used by attackers to get more permissions in the environment, commonly known as lateral movement.	All Accounts	2 Accounts | 21 Findings ›	✉	0 Identities
Unusual Reconnaissance An identity that is collecting information about the environment while it has no history of performing similar actions. This is a common technique used by attackers to identify who has access to what and identify sensitive data.	All Accounts	2 Accounts | 21 Findings ›	✉	0 Identities

Detect anomalies and investigate unusual behavior, including reconnaissance, across data, network and permissions

Ermetic for cloud security posture management

Ermetic offers CIEM and robust CSPM in one, fully integrated platform. It lets you manage your cloud asset inventory and compliance from a single pane of glass– and drill down into and auto-remediate misconfigurations. The platform tracks how your organization scores against common industry standards and best practices including: GDPR, NIST, PCI DSS, HIPAA, ISO, SOC 2, AWS Well-Architected and CIS for AWS and Azure.



Standard	Summary
AWS Well Architected - Key concepts, design principles, and architectural best practices for designing and running workloads in the cloud	58%
CIS AWS 1.3.0 - An objective, consensus-driven security guideline for the Amazon Web Services cloud provider	31%

Requirement	Summary
1. Identity and Access Management	33%

Requirement	Summary
1.4 Ensure no root user account access key exists The root user account is the most privileged user in an AWS account. AWS Access Keys provide programmatic access to a given AWS account. It is recommended that all access keys associated with the root user account be removed.	50%
1.5 Ensure MFA is enabled for the "root user" account The root user account is the most privileged user in an AWS account. Multi-factor Authentication (MFA) adds an extra layer of protection on top of a username and password.	0%
1.7 Eliminate use of the root user for administrative and daily tasks The root user has unrestricted access to and control over all resources in the AWS account. It is highly recommended that the use of this account be avoided for everyday tasks.	50%
1.8 Ensure IAM password policy requires minimum length of 14 or greater IAM password policies can be used to ensure password are at least a given length. It is recommended that the password policy require a minimum password length 14.	25%
1.9 Ensure IAM password policy prevents password reuse IAM password policies can prevent the reuse of a given password by the same user. It is recommended that the password policy prevent the reuse of passwords.	25%
1.10 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password Multi-Factor Authentication (MFA) adds an extra layer of authentication assurance beyond traditional credentials. It is recommended that MFA be enabled for all accounts that have a console password.	3%
1.12 Ensure credentials unused for 90 days or greater are disabled AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys. It is recommended that all credentials that have been unused in 90 or greater days be deactivated or removed.	28%
1.14 Ensure access keys are rotated every 90 days or less Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS. It is recommended that all access keys be regularly rotated.	61%

Detect misconfigurations, track compliance and report on your cloud security posture improvements

Conclusion

The complexity of public cloud infrastructure makes understanding the risk to your organization extremely difficult. Ermetic is an award-winning identity first cloud security solution that offers leading cloud infrastructure entitlement management and cloud security posture management in one platform, through a single pane of glass. Organizations use Ermetic to reduce their cloud attack surface and blast radius while reducing time and costs -- and amplifying cloud security expertise for security and engineering teams.

Ermetic is the only solution in its category to offer full-stack insight into entitlements across identities, compute resources, data stores and the network. This comprehensive view enables you to investigate deeply what is going on in your cloud infrastructure at any given time. Ermetic helps you secure your cloud infrastructure effectively and automate least privilege based on actual use.

Version 2 [January 2022]

www.ermetic.com