ermetic

Identity-First
Cloud Infrastructure Security

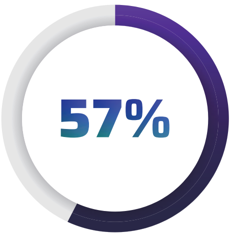
Holistic, multicloud protection across identities, data, network and compute resources

Reduce Your Cloud Attack Surface

One of the most underestimated risks to cloud infrastructure -- and the hardest to find and fix -- is misconfigured identities. By 2023, identities and privileges will be the cause of 75% of cloud security failures [Gartner]. To successfully manage your cloud security posture, you need to go deep on identities.

Of large companies cite access as a primary root cause of their cloud data breaches

Of organizations spend more than 25 hours weekly on cloud infrastructure IAM



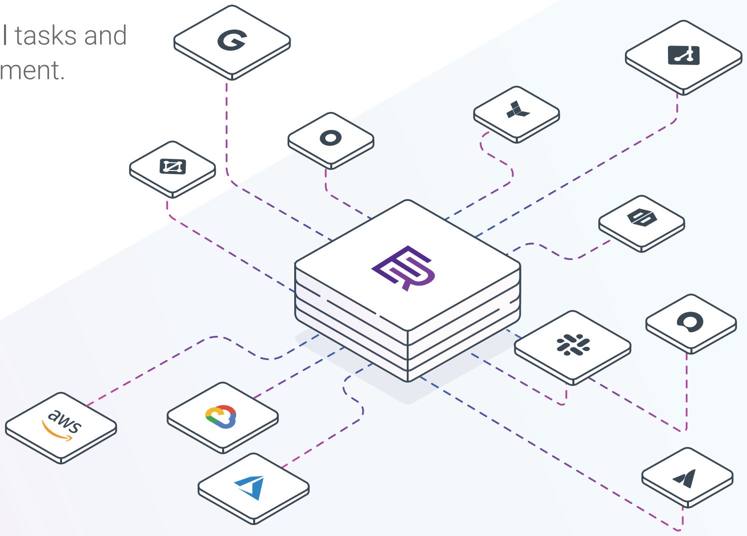
Of enterprises cite lack of visibility and inadequate IAM as major cloud security threats

Security and Compliance across AWS, Azure and GCP

Ermetic is an identity-first solution for securing cloud infrastructure at scale. It combines a full lifecycle approach for entitlements management (CIEM) and security posture management (CSPM) to detect, reduce and prevent risks to cloud assets, through:

- A full SaaS platform that offers fast value and is easy to operationalize and use
- Actionable and granular visibility into all multicloud assets
- Risk findings of exceptional depth, prioritized by severity
- Built in remediation steps based on actual-use least privilege
- Automated security posture management and compliance
- Access governance with full control over sensitive resources

Ermetic is a force multiplier for Security, reducing manual tasks and improving communication with DevSecOps and management.



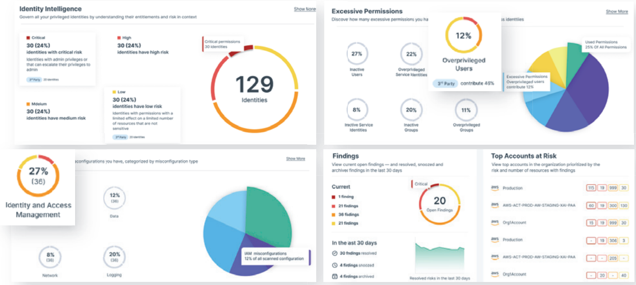
CIEM and CSPM in One

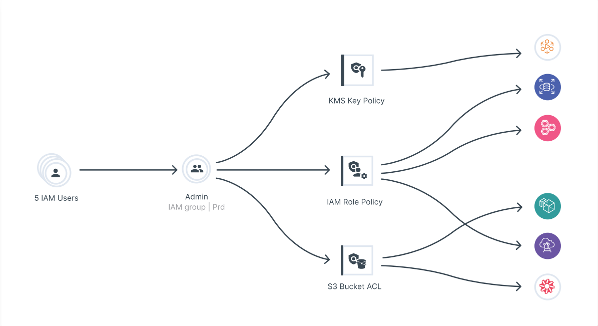
Cloud Infrastructure Entitlements Management and Cloud Security Posture Management in one unified platform

SEE.

Actionable visibility and multi-cloud inventory management

Start from the dashboard and drill down/query into permissions, configurations, network and activities -- for the full range of cloud resources.


Identity Intelligence
Govern all your privileged identities by understanding their entitlements and risk in context
Show More
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
Critical permissions
30 identities
129
Identities
Excessive Permissions
Show More
27%
Inactive Users
22%
Overprivileged Service Identities
12%
Overprivileged Users
3rd Party
contribute 46%
8%
Inctive Service Identities
20%
Inactive Groups
11%
Overprivileged Groups
Used Permissions
25% Of All Permissions
Excessive Permissions
Overprivileged users contribute 12%
27%
(36)
Identity and Access Management
Show More
12%
(36)
Data
8%
(36)
Network
20%
(36)
Logging
IAM misconfigurations
12% of all scanned configuration
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
Critical
20
Open Findings
In the last 30 days
30 findings resolved
4 findings snoozed
4 findings archived
Resolved risks in the last 30 days
Top Accounts at Risk
View top accounts in the organization prioritized by the risk and number of resources with findings
Production
AWS-ACT-PROD-AW-STAGING-XAI-PAA
Org1Account



ACT.

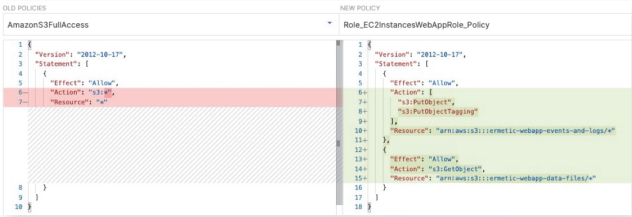
Visual risk assessment across identities, network, compute and data

Gain full stack insight into excessive and risky permissions, network exposure, misconfigured resources, sensitive data and vulnerable workloads.

COLLABORATE.

Automated and tailored remediation

Mitigate risk efficiently using auto-generated -- and customizable -- policies based on actual activity. Integrate them easily across ticketing, CI/CD pipelines, and IaC and other workflows.



OLD POLICIES

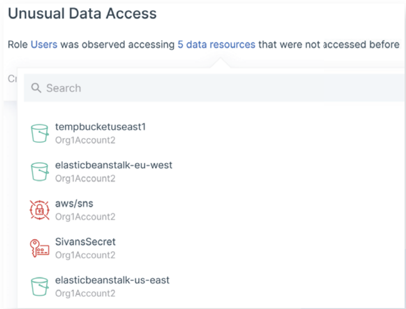
AmazonS3FullAccess

```
{
  "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/*"
    }
  ]
}
```



Unusual Data Access

Role Users was observed accessing 5 data resources that were not accessed before

Search

tempbucketuseast1
Org1Account2

elasticbeanstalk-eu-west
Org1Account2

aws/sns
Org1Account2

SivansSecret
Org1Account2

elasticbeanstalk-us-east
Org1Account2

INVESTIGATE.

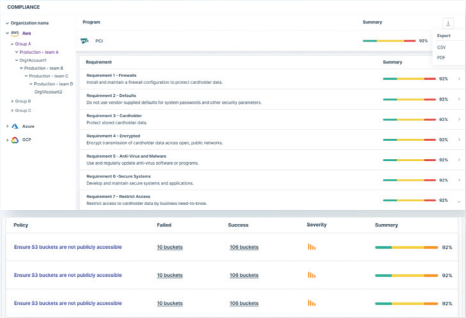
Anomaly and threat detection

Apply advanced behavioral analytics against baselines to discover identity-based anomalies and threats, including unusual reconnaissance, configuration changes and suspicious data access.

COMPLY.

Compliance and access governance

Ensure compliance with industry standards including CIS, GDPR, HIPAA, ISO, NIST, PCI and SOC2, and define your own custom policies. Audit and investigate activity with contextual visibility into enriched access logs.



COMPLIANCE

Program	Summary
PCI	92%

Requirement	Summary
Requirement 1 - Firewalls Install and maintain a firewall configuration to protect cardholder data.	92%
Requirement 2 - Defaults Do not use vendor-supplied defaults for system passwords and other security parameters.	92%
Requirement 3 - Cardholder Protect stored cardholder data.	92%
Requirement 4 - Encrypted Encrypt transmission of cardholder data across open, public networks.	92%
Requirement 5 - Anti-Virus and Malware Use and regularly update anti-virus software or programs.	92%
Requirement 6 -Secure Systems Develop and maintain secure systems and applications.	92%
Requirement 7 - Restrict Access Restrict access to cardholder data by business need-to-know.	92%

Policy	Failed	Success	Severity	Summery
Ensure S3 buckets are not publicly accessible	10 buckets	106 buckets		92%
Ensure S3 buckets are not publicly accessible	10 buckets	106 buckets		92%
Ensure S3 buckets are not publicly accessible	10 buckets	106 buckets		92%

*IDC State of Cloud Security 2021 Survey, commissioned by Ermetic

To learn more or schedule a demo, contact: info@ermetic.com

ermetic