ermetic | Industry Brief

Financial Services – Securing Identities in Your Cloud Infrastructure with Ermetic

Financial Services - Securing Identities in Your Cloud Infrastructure with Ermetic

Financial organizations are adopting the cloud at a rapid pace. A robust cloud security solution for securing identities will ensure you reap the benefits.

The finance industry is a strong adopter of public cloud – 83% of financial services companies are already using the public cloud in some form.* The cloud's many benefits can help reduce costs, drive innovation, meet customers' digital expectations – and even enhance security.

As financial institutions migrate to the cloud, they encounter a new world and new set of security challenges. For starters, they are the primary target of cyber attackers – with ransomware, supply chain attacks and digital vulnerabilities ranking as the most serious threats. Attackers typically use exploitation patterns designed at breaching infrastructure and gaining access to high-value assets. Almost every cloud data breach – both its enablement and its amplification – involves misconfigured infrastructure or a compromised identity, service or human, and their permissions to access resources.

The move to the cloud gives you an opportunity to implement effective cloud security from the start. First, you must be aware that the greatest risk to your cloud environment is misconfigured identity – with network security and workload vulnerabilities runners-up as the second- and third-ranked risks. To address this top risk – and have a true understanding of your cloud environment's security posture – you must have granular visibility into the access granted every identity and to every resource, and the actual use of that access. Such visibility is the cornerstone of building least privilege across your entire cloud infrastructure, reducing your attack surface.

Ermetic shows risk findings with surgical precision and provides actionable steps for fixing them. Financial organizations worldwide use Ermetic to easily and expertly manage identity and access risk, ensure compliance and drive least privilege across their multicloud environment.

Cloud Security Challenges of Financial Institutions

Financial organizations need an effective cloud security implementation because they manage large volumes of sensitive information, need to comply with strict industry standards and are the top pick of attackers.They must also cope with the challenges all industries face in the cloud.

Finance is the primary target for cyberattackers

96%	USD 5.97M	200%
of data breach motives in North America were financial Source: Verizon 2022 Data Breach Investigations Report	Average cost of a data breach in financial orgs Source: IBM Cost of a Data Breach 2022	Increase in # of times/year the FS-ISAC raised the threat level compared to the two previous years Source: Financial Services Information Sharing and Analysis Center, 2021

Regulator-induced challenges

With its large volumes of confidential customer and other sensitive information, the finance industry must adhere to strict industry standards and best practices for protecting data in the cloud. The fragmented nature of financial regulatory bodies makes reviews and approvals hard to attain. A Google and Harris Poll survey of financial services institutions found that more than a third (38%) of on-premises respondents were not using cloud services due to the immense investment of resources required for the regulatory approval process.*

Rushed cloud adoption

Finance entities are accelerating their migration to the cloud, development at breakneck speed even as migration is underway. Yet rushed cloud adoption – and new environments brought in by mergers and acquisitions – can lead to risky

implementation if cloud security best practices are lacking. For example, failure to effectively monitor or resolve misconfigurations, or excessive granting of permissions that may seem harmless, can widen your cloud attack surface and, upon a breach, potential damage from lateral movement. Security teams report the difficulty of standardizing or collaborating on security across different product groups, augmented by a lack of visibility into the cloud environment for all.

Cloud vs on-prem

Agile, developer-centric and business-driven, the cloud is different from on prem – and so is securing it. Its attack vectors span IAM, network, workloads and data. Identity is the new perimeter, making misconfigured identities and privileges the greatest risk to the cloud environment.

> By 2023, 75% of security failures will result from inadequate management of identities, access, and privileges
>
> [Gartner]

At any given time, a cloud environment is using hundreds of policies and configurations, coupled with tens of thousands of service identities, and human identities, all with privileges to resources. Just one excessive permission is enough for an attacker to take over the entire environment. Without secure access management, identities can be easily breached. To implement least privilege, as required by cloud security best practice. You need to know which identities can access which resources and if the permissions are in use; if you don't know this, your environment is not secure and not compliant.

Lack of granular visibility

Cloud complexity creates a lack of visibility into excessive permissions and other access-related risks. Securing identities and entitlements in cloud infrastructure with native tools is an impossible task – the tools require much work, are hard to scale and do not support multicloud environments. To effectively determine access risk, a solution needs to use more than simply the APIs of cloud providers to visualize the data – this approach is superficial and the findings it reveals are not usable. Actionable visibility requires a solution built with deep understanding of the mechanisms of each cloud provider's infrastructure and permissions model.

Short on cloud expertise

Many organizations at an early stage of cloud maturity – and even those farther along – are challenged by a lack of cloud and cloud security experience among their teams. Widespread digital transformation including remote work has created a worldwide demand for cloud professionals proficient in AWS, GCP, Azure, Kubernetes and different areas of cloud security. Today, financial and other organizations are struggling with a shortage of the cloud knowledge and skills set essential to properly building, maintaining, innovating and securing a cloud environment.

Shared responsibility with cloud providers

The shared responsibility model is a cloud security framework defined by cloud providers that determines which cloud components are the cloud provider's responsibility to secure and which are the customer's. While aimed at providing clarity, the model is often confusing, especially for professionals taking their first steps in cloud security. As a rule, the cloud customer bears responsibility for securing their data in the cloud.

Ermetic - Unique Value for Financial Services Institutions

Ermetic is a comprehensive cloud security platform for AWS, Azure and GCP that enables financial entities to prevent breaches by reducing the attack surface of their cloud infrastructure and implementing least privilege access at scale in even the most complex environments. Ermetic holistically enables risk assessment across the entire security stack – from full asset discovery and deep risk visualization, prioritization and guided remediation to anomaly detection and compliance audit, from runtime to production.

Of all risks, identity-related toxic permissions scenarios are the highest. This is because even one misconfiguration is enough for a bad actor to take over. Yet, a stark reality exists: Almost all configured permissions for services and applications running in an organization's cloud environment – including for financial institutions – are excessive.

Ermetic's identity-first platform uniquely detects, prioritizes and mitigates these hard-to-find risks. Built into Ermetic is years and layers of understanding of the mechanisms and permissions models of different cloud provider infrastructures. The platform identifies the actual use of granted permissions to provide precise and

conservative policy recommendations for the set of permissions needed for a given function and no more. Ermetic facilitates mitigation by integrating these optimized policies and configuration fixes in your workflows, CI/CD pipelines and infrastructure as code.

Ermetic brings financial organizations further value through actionable visibility and ease of use that reduces overhead for all cloud skill levels and democratizes cloud security across all stakeholders.

Ermetic - Capabilities

Ermetic offers holistic cloud infrastructure security that includes cloud identity entitlements management (CIEM), cloud security posture management (CSPM) and other capabilities in one platform, to provide industry-leading:

- Multicloud inventory management
  - Manage the full range of cloud resources across permissions, configurations, network and activities
- Full-stack risk assessment across identities, network, compute and data
  - Reveal excessive permissions, network exposure, misconfigured resources, sensitive data and vulnerable workloads. Enforce least privilege with Just in Time access for developers.
- Automatic remediation tailored to your needs
  - Mitigate risk efficiently using auto-generated policies based on actual activity and integrated across ticketing, CI/CD pipelines, and IaC and other workflows
- Policy enforcement & shift left
  - From development to production, define and enforce automated guardrails for access permissions and resource configuration
- Anomaly and threat detection
  - Detect suspicious behavior and configuration changes with continuous behavioral analysis. Investigate incidents including session monitoring with visibility into enriched access logs.
- Compliance & access governance
  - Continuously audit inventory and compliance including PCI-DSS, NIST, CCPA, GDPR, SOC2, ISO and CIS. Generate reports including for asset inventory, network configurations and activity audits.

Next Steps

Securing cloud infrastructure to fend off attackers pursuing the sensitive data of financial organizations requires a new mindset. Of all the risks, misconfiguration around identity and access management is the greatest. Conventional IAM solutions solve for employee permissions, not the permissions of service identities. You may not be aware you have this problem, but you and every organization using the cloud does. Wherever you are on your journey to the cloud, prioritize implementing a solution that provides deep, granular visibility as the cornerstone of the least privilege needed to effectively secure your cloud infrastructure.

Ermetic offers financial organizations comprehensive cloud infrastructure security and compliance built from the ground up to uniquely identify risky access and misconfigurations that matter the most, and provide usable fixes easy to implement - reducing risk and saving security stakeholders hours and days of time. Using Ermetic you can incorporate the deep visibility and precise assessment of access use and risk that is essential to establishing the least privilege that is essential to implementing your zero trust strategy. Ermetic also offers an incremental approach for strategically advancing your organization to greater cloud security maturity.

What Ermetic FinServ Customers Are Saying

> By enabling us to jump through our cloud security audit hoops near effortlessly, Ermetic has proved itself a capable technology and time saver — and is actually helping us grow the business.
>
> [Etienne Smith, CTO, Kikapay]

> Ermetic plays a big role in helping verify if our security profile is good enough for addressing our [Financial Conduct Authority - FCA] compliance obligations.
>
> [Leo Thesen, Senior Engineer and Security Technical Lead, MOHARA]

About Ermetic

Ermetic enables financial service organizations to prevent breaches by reducing the attack surface of cloud infrastructure and enforcing least privilege at scale in the most complex environments. The Ermetic SaaS platform provides comprehensive cloud security for AWS, Azure, and GCP that spans both Cloud Infrastructure Entitlements Management (CIEM) and Cloud Security Posture Management (CSPM). The company is led by proven technology entrepreneurs whose previous companies have been acquired by Microsoft, Palo Alto Networks, and others. Ermetic has received funding from Accel, Forgepoint, Glilot Capital Partners, Norwest Venture Partners, Qumra Capital, and Target Global.

Visit us at https://ermetic.com/ and follow us on LinkedIn, Twitter, and Facebook.

* Google Cloud and Harris Poll survey, 2021