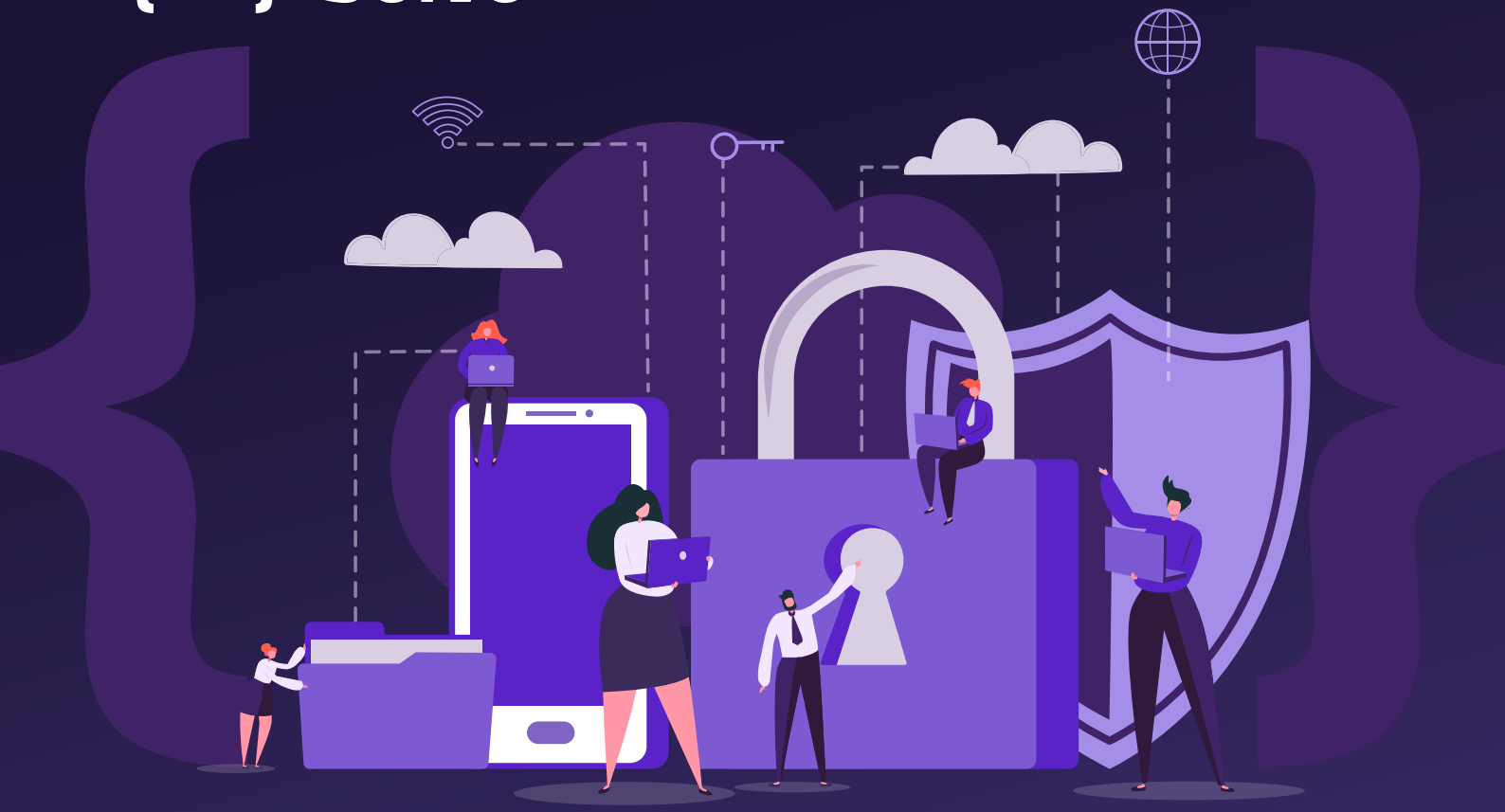
{ Solvo



Adaptive Cloud Security for Retail Digital Transformation

Driven by the rapid adoption of cloud computing as well as changes to both life and work habits in the aftermath of the COVID-19 pandemic, retailers are transforming the way they engage, interact, and support their customers.

These changes are taking place across the entire retail ecosystem:

E-commerce companies continue to challenge traditional retail models, creating personalized, digitally enhanced shopping experiences.

At the same time, established brick-and-mortar retailers are boosting their online presence while bringing digital innovation into physical stores.

{☁} Solvo

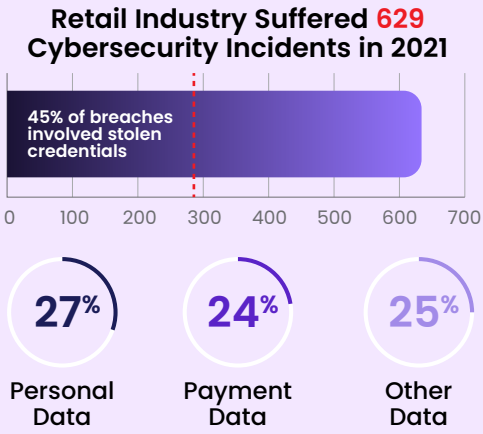
Retail digital transformation revolves around the ability to quickly respond to changing customer needs and market conditions. As retailers evolve towards digital-first businesses, they're becoming increasingly dependent on cloud infrastructure to provide them with the agility and resiliency required to bring better products to market faster. In addition, retailers are using the cloud to store and analyze vast amounts of data about customers, inventory, transactions and more to gain competitive advantages and operational efficiencies, and improve customer experience.

Cloud security challenges for retailers

The adoption of cloud services brings new challenges to retailers. Over the last several years , the retail industry has become a primary target for attackers. By hacking into a retailer's public infrastructure, cyber criminals can gain access to a treasure trove of sensitive information such as credit card and social security numbers, bank accounts, and other personally identifiable information (PII).

According to Verizon's **2022 Data Breach Investigations Report,** the retail industry suffered 629 cybersecurity incidents in 2021, including 241 with confirmed data disclosure. 45% of these breaches involved stolen credentials, followed by personal data (27%), other (25%), and payment (24%) data. These statistics show the extent to which retailers are exposed to data breaches, which is largely attributed to the expanded attack surface created by the shift to cloud infrastructures and digital supply chains connecting suppliers and customers.

While the major public cloud providers offer robust security capabilities, the shared responsibility model requires customers to protect their own data and applications in the cloud. However, defining appropriate access policies and controls to protect sensitive data is a challenging task.



Least privilege requires continuous visibility

Ideally, secure access to cloud environments can be achieved through the least privilege model, where users or roles are only granted the minimum level of access permissions necessary to do their jobs.

Implementing an effective least privilege model requires continuous, real-time visibility into cloud infrastructure configuration changes that impact an ever-growing number of entities. Otherwise, excessive or unnecessary permissions will go unnoticed and may be exploited by attackers. On the other hand, applying overly strict least privilege permissions across the board to protect against the unknown may cause disruption to legitimate business operations.

Many retailers struggle to apply an effective least privilege approach due to the difficulty of continuously validating and updating IAM configurations and policies across cloud environments that keep growing in size and complexity. In accordance, Verizon's report pointed out that misconfiguration errors are a primary cause for retail data breaches involving PII. Misconfiguration errors are often a result of failing to define appropriate access controls to cloud data stores.

Moreover, the report notes that "data tends to be from customers, and it is also the customers who are notifying the breached organizations in a high number of cases." This suggests that companies lack adequate visibility into their cloud environments to monitor access and use of sensitive data and systems and detect breaches.

{ Solvo }

When things get out of control

The lack of cloud access visibility is related to the fact that cloud infrastructures tend to grow out of control very quickly. The flexibility of the cloud and the ease of provisioning resources may turn a retailer's cloud infrastructure into a very chaotic environment with multiple users requiring access to an ever-expanding range of cloud resources and services. In addition to human identities, machine accounts are frequently created for multiple entities, many of which have a lifespan of only a few days or hours.

Given the size and complexity of these environments and their dynamic nature, it's becoming difficult to keep track of changes, estimate risks, and define access policies and permissions accordingly. This process has to be repeated over and over again, especially when dealing with multi-cloud deployments. In this state of things, it's almost inevitable that errors will occur - either misconfigured entitlements, privileged accounts left unused, or overly excessive permissions that were not detected in a timely manner - and become vulnerabilities that attackers are actively looking to exploit.

In addition, retailers are adopting agile methodologies such as CI/CD to expedite the development and deployment of advanced cloud-enabled services. Unless properly secured, faster release cycles may increase the risk of exposing secrets such as passwords, database credentials, API keys, and security tokens in the source code.

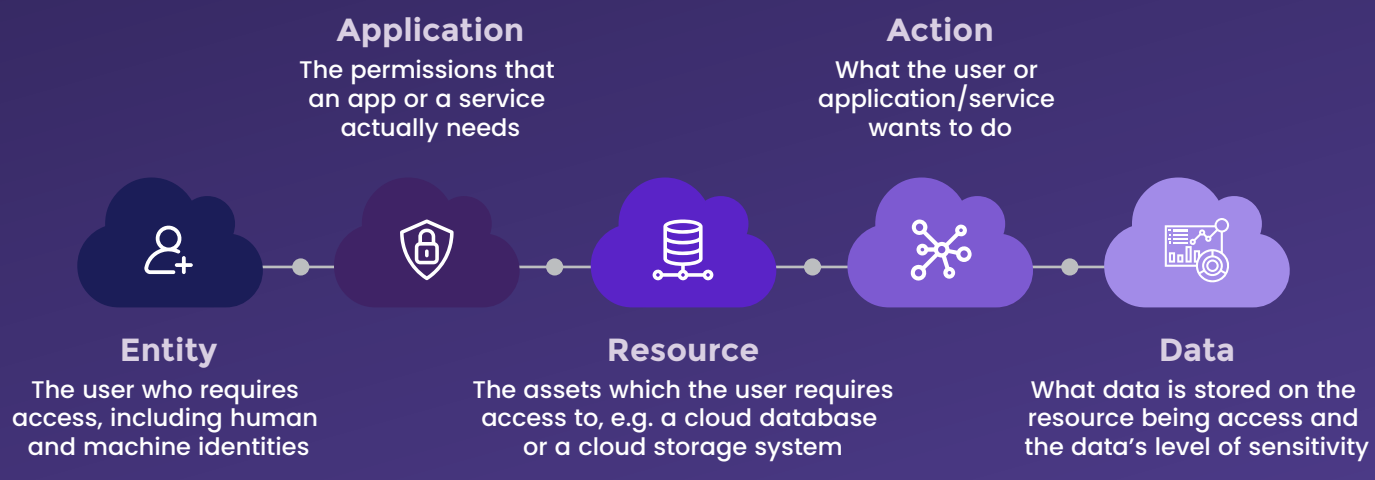
Mitigating access risks with automation and contextualization

The key for gaining control over access to cloud environments, and implementing effective least privilege policies is to reduce the need to constantly define, redefine and enforce policies and controls. Ideally, this could be done by automating the processes of monitoring, identifying and mitigating cloud access risks based on their severity.

However, automation must be based on continuous and deep understanding of the access landscape, which can be leveraged to create access policies and entitlements that are consistent with the level of estimated risk. To accomplish that, automation should be strongly coupled with contextualization.

The missing piece in traditional identity and access management approaches, where permissions are granted based on users' roles and responsibilities, is context. In today's dynamic cloud environments, with so many moving parts in play, permissions and entitlements should be based on a broader, contextual understanding of user activities and not rely solely on static roles. This would enable retailers to assess risk in a more accurate manner, and automatically apply policies and entitlements that reflect the real level of threat.

Contextual understanding along these lines requires visibility into several dimensions:



Solvo

By gaining visibility and constantly analyzing configurations, relationships, and activities across these dimensions, retailers can identify and mitigate vulnerabilities in a timely manner.

They can prioritize risk and automatically apply the right policies and entitlements on an ongoing basis while reducing the operational burden on security teams and developers.

Solvo's adaptive cloud infrastructure security

Solvo takes a different approach to cloud security that enables retailers to digitally transform and grow their business in a secure manner.

Solvo enables security teams, developers and other stakeholders to automatically uncover, prioritize, mitigate and remediate cloud infrastructure access risks. Using multi-dimensional, contextual monitoring and analysis of infrastructure resources, applications and user behavior, and the data associated with them, Solvo enables enterprises to implement adaptive least privilege access policies and controls at scale.

Solvo automatically creates customized, constantly-updated least privilege access policies based on the level of risk associated with entities and data in the cloud. Solvo helps CISOs identify and prioritize risks, and proactively mitigate cloud misconfigurations and vulnerabilities while facilitating collaboration between security, DevOps and engineering teams. Using Solvo, retailers can reduce their cloud attack surface, simplify compliance, and grow their business in a secure manner.

By breaking down application, identity and data silos, Solvo offers a first-of-its-kind application and data-aware cloud infrastructure security platform designed for the scale and speed of cloud-native environments.

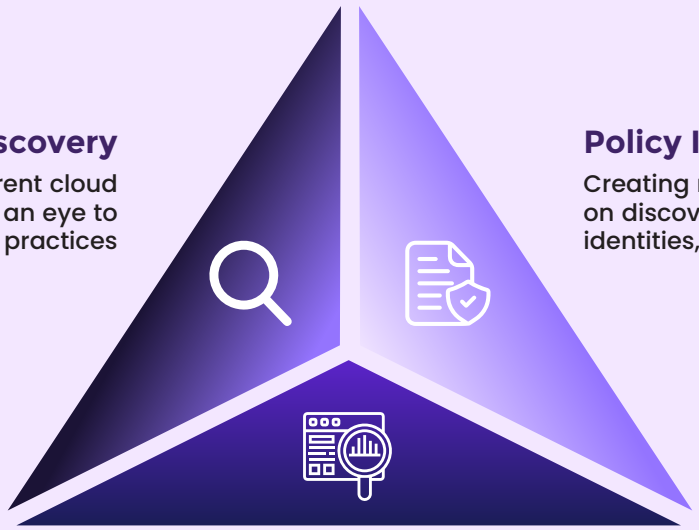
Solvo's unique platform gets to work right away in three distinct stages:

Discovery

Analyzing the current cloud environment with an eye to best practices

Policy Implementation

Creating new security policies based on discovered access, accounts, identities, and entitlements



Enforcement

Monitoring application and data changes and updating access policies in real time; automatically creating new policies when new code or resources are added

Solvo

Avoiding the consequences of retail cloud data breaches

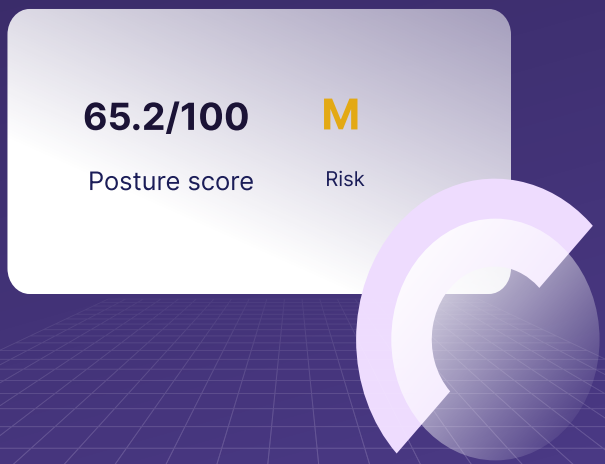
The costs of a retail data breach may go far beyond the immediate damage, which can be measured in system downtime, clean up cost, etc. Perhaps more than any other industry, retailers are highly dependent on their reputation. In the e-commerce age, consumer loyalty is eroded. In case of a data breach, concerned consumers can quite easily replace their supplier, resulting in significant impact on the bottom line.

In the longer term, retailers that have suffered sensitive data breaches will be faced with additional consequences, such as having to provide compensation to customers. Even more importantly, as an industry that deals with PII, retailers are becoming subject to fines and legal actions for non-compliance with privacy regulations such as PCI DSS and GDPR.

Using Solvo, retailers can implement a proactive approach to mitigating cloud access risks that can adapt to the frequent changes in distributed and complex cloud infrastructures. Solvo's contextual, multi-dimensional analysis enables retailers to restrict access to sensitive data per deep and dynamic granularity-based need, and improve secret management through IAM roles.

Sign up today for an up-close demo of what Solvo can do to help you take care of cloud security - and start getting all your teams on the same page.

SecurityGenie™



Key benefits

- Comprehensive visibility into your cloud infrastructure inventory
- Create customized, automatically updated least privileged access policies based on the level of risk associated with entities, resources, applications and data in the cloud
- Proactively monitor, identify, prioritize and remediate the most critical risks to your cloud infrastructure
- Minimize cloud security alert fatigue and false positives
- Reduce your cloud attack surface to innovate and grow your business in a secure manner
- Create stronger alignment and improved collaboration between security, DevOps and engineering teams
- Simplify compliance and reporting