aws | Aporeto
Zero Trust Cloud Security

Aporeto and Amazon Web Services

Case Study | Informatica

Informatica Eliminates SSH Key Management with Aporeto Cloud PAM on AWS

"With Aporeto's Cloud PAM, I have eliminated the need for SSH key management. I can leverage our identity provider to enable users with SSO authentication and authorization while maintaining control with just-in-time access to instances. All user activity is logged, simplifying Informatica's ability to meet compliance, conduct audits and making my job a whole lot easier overall."

Alec Chattaway

Director of Cloud
Infrastructure Operations

Informatica

About Informatica

Informatica is a leader in Enterprise Cloud Data Management, providing solutions that help organizations optimize, transform, and analyze their data. Informatica's Intelligent Data Platform is built on a microservices architecture, helping organizations ensure their data is trusted, secure, governed, accessible, timely, relevant, and actionable on-premises or on the cloud.

Challenges

With more than 10,000 instances and containers, Informatica struggled to apply consistent security policies to manage administrative secure shell (SSH) access to their infrastructure across their on-premises and cloud environments. Previously, Informatica spun up new instances but instead of issuing a new SSH key per user to access instances, they were initially allowing groups to share keys which went against their compliance standards. To mitigate this risk, they restricted and rotated keys between users, which quickly became complex and inefficient. This led to Informatica operating with multiple security interfaces, making it difficult to track who could access their instances, and from where.

Additionally, as Informatica was developing new processes and applications, they were finding it increasingly difficult to map application dependencies between instances and container workloads. Because of this, Informatica was looking for a solution that would provide them with comprehensive visibility and better control over their sprawling environment.

Why Aporeto

To improve compliance controls for their hybrid cloud infrastructure, Informatica created a new CloudTrust team. As the team evaluated different solutions, they had to consider

Benefits:

- Increased consumption and security of AWS services
- Reduced application deployment times by 200 hours
- Eliminated need for prescheduled downtime windows
- Improved security of 10,000 to 20,000 instances and containers on AWS environment

whether they were going to build or buy, and how they could evolve their security model from an on-premises design, to an agile, cloud-specific design. Over the course of six months, the team evaluated potential third-party solutions as well as created their own Proof of Concept (PoC) for an internal solution. The internal solution was not sustainable, as it required significant resources in order to maintain it post development. After evaluating all the third-party solutions, Informatica chose Aporeto based on its unique approach to cloud security that is centered around application identity. Aporeto's identity-based approach to cloud security removes complexity by providing Informatica with the ability to easily scale their application architecture, automate policy distribution and enforcement for both on-premises and cloud workloads, and the ability to leverage their existing identity provider (IdP) to control user access to servers and applications.

The Solution

Initially Informatica engaged with Aporeto to solve their network security policy distribution and enforcement challenges, but soon expanded the focus of their engagement to also include a powerful and simplified approach to manage administrative access to infrastructure. Having consistent policy management and proper access control is critical to Informatica's operations. With Aporeto, Informatica realized they could track, block, and audit user access throughout their infrastructure, as well as provide "keyless" access to Amazon Elastic Compute Cloud (Amazon EC2) instances. Aporeto's Cloud Privileged Access Management (PAM) provides keyless access through just-in-time, single sign-on (SSO) for SSH access, while also logging all associated activity for compliance purposes.

Aporeto worked with the Informatica team to run a PoC demonstrating how Aporeto's unique approach to microsegmentation using identity, not IP addresses, creates an inherent Zero Trust model contributing to a defense in depth security approach. Each workload is extracting information in the form of metadata, labels and tags to generate a cryptographic identity. From this identity, Aporeto creates security policies that are portable and persistent regardless of where the workload resides. Aporeto distributes security policies to the Aporeto Enforcer (agent) that sits on the host, enabling the workload to authenticate and authorize app to app, or user to app communication, otherwise no connectivity is allowed. This centralized policy management and distribution enables the Informatica team to deploy harmonized security at the app level across workloads or microservices including Amazon EC2, Amazon Elastic Containers Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and AWS Lambda with API access control. Aporeto provides hybrid cloud security without relying on static network segmentation, access control lists (ACLs), or IP addresses.

After a successful PoC, the team moved onto addressing another significant priority – SSH and secure data access. Informatica selected Aporeto's Cloud Privileged Access Management (PAM) to eliminate the need for SSH keys altogether by replacing keys with ephemeral SSH client certificates provided by Aporeto. With this new approach, Informatica is able to provide just-in-time (JIT) access for any user to Linux instances where policies are time based. This provides SSO authentication and authorization based on the user claims that reside in the identity provider (IdP) to control access to Linux workloads across hybrid and AWS environments. Aporeto embeds each user's unique identity into each certificate which allows Informatica to not only control access, but maintain audit logging with command line access to see what functions a user performed and when. This approach greatly simplifies compliance and improves audits and forensics.

In addition, Aporeto provides Informatica with visibility into their environment that they did not previously have. This allows them to view common patterns vs. anomalies that can be vulnerabilities or potential attacks, for quick remediation. Doing so has strengthened the security, reliability, and resiliency within Informatica's environment.

The Aporeto Platform Architecture

The Aporeto platform consists of two components, the Security Orchestrator and Enforcer. The Aporeto Security Orchestrator functions as the control panel and is responsible for workload and infrastructure identity management and the policy engine. From here, policies are distributed to all the individual workloads. The Security Orchestrator has powerful APIs that allow the Aporeto platform to integrate seamlessly with a broad set of enterprise platforms into the entire infrastructure, from CI/CD pipeline to user SSO, to security operations center.

The Aporeto Enforcer is deployed as either a container or as an enforcement node on an individual host or VM. Any workload outfitted with the Enforcer and working in conjunction with the Orchestrator, is enabled with automated issuance and management of security policy at different layers of the stack. Enforcers implement functions that include threat monitoring, transparent network security, API authorization, and authentication. The Aporeto platform enables comprehensive security management across heterogeneous infrastructure and any workload for a Zero Trust security posture.

Benefits

With Aporeto, Informatica built a robust security posture on AWS to meet their stringent compliance requirements, all while accelerating consumption of cloud infrastructure to meet business needs. This has resulted in dramatic time savings and operational efficiency. By automating the authentication process, Informatica has seen their development cycles decrease drastically as developers no longer have to manually insert the two-factor authentication into the code and approve it. The total resource hours for deploying a new application to AWS has gone down by 200 hours and the average deployment time has gone down from six months to just under one month.

The benefits that Informatica's engineers have seen also trickled down to its customers. Informatica's customers are enjoying increased product resiliency since the deployment of Aporeto. Informatica has prescheduled windows of downtime throughout the month for new deployments, which due to Aporeto, has decreased from eight hours to four hours per month with most deployments not actually requiring any downtime at all.

As an additional benefit, Aporeto has allowed Informatica to increase their usage of Amazon Web Services (AWS) and take advantage of the services they didn't have the resources for prior. Of those services, Informatica found great value in investing more heavily into Amazon EKS to simplify control plane and container deployment management across all their environments. Access to the control plane services from any instance is now controlled by Aporeto's Cloud PAM solution. By utilizing the Amazon EKS orchestration service, Informatica has reduced resource consumption of instances by about 60% along with a reduction in automation complexity to access these services. By combining Amazon EKS with Aporeto, access to worker nodes can be controlled via Aporeto's Cloud PAM SSH module. This allows for fine-grained user access to the containers themselves in addition to complete audit capabilities which were previously unavailable.

AWS services Informatica leverages:

- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Containers Service (Amazon ECS)

Next Steps

Informatica is always looking for ways to add new features and improve the experience for both their internal teams and customers. Part of this includes creating specific, policy-based controls and automating those policies. They are looking to Aporeto to help with this by adding the equivalent AWS security groups to each deployment, which would provide a duplicate set of controls to help them maintain compliance.

About Informatica

Informatica is the only proven Enterprise Cloud Data Management leader that accelerates data-driven digital transformation. Informatica enables companies to fuel innovation, become more agile, and realize new growth opportunities, resulting in intelligent market disruptions. Over the last 25 years, Informatica has helped more than 9,000 customers unleash the power of data. For more information, call +1 650-385-5000 (1-800-653-3871 in the U.S.), or visit **www.informatica.com**.

Informatica

Aporeto

Zero Trust Cloud Security

About Aporeto

Aporeto, the leader in Zero Trust Cloud Security, provides comprehensive network security through microsegmentation and secure access to applications and infrastructure using application identity rather than IP addresses. The Aporeto SaaS-based platform allows you to build and enforce distributed identity-based policies enabling authentication, authorization, and encryption across all workloads including containers, Kubernetes, serverless, service mesh and VM environments. Aporeto protects against attacks and enables complete visualization, simplified proof of compliance, centralized management, and accelerated app migration. Aporeto future proofs your infrastructure, delivering stronger cloud security, operational agility to accelerate digital transformation, and better ROI for any infrastructure at any scale. Learn more at **www.aporeto.com**.

Check out the **Aporeto AWS Marketplace Page** for more information.

CONTACT US
Aporeto
10 Almaden Blvd., Suite 400
San Jose, CA 95113
www.aporeto.com

For a demo or free trial please contact Aporeto Sales:
833-276-7386 or **415-730-0159**