Check Point
SOFTWARE TECHNOLOGIES LTD

CASE STUDY

PACIFIC LIFE

"CloudGuard Dome9 is a huge force multiplier, providing tools that are highly effective and efficient. Because CloudGuard Dome9 is enabling our cloud strategy, we can innovate and offer better products, while lowering our expense ratio, giving customers better value."

Reza Salari
Manager of Information Security and Telemetry, Retirement Solutions Division

PACIFIC LIFE

CLOUDGUARD DOME9, HELPING PACIFIC LIFE STREAMLINE SECURITY COMPLEXITY IN THE CLOUD

ABOUT PACIFIC LIFE

Pacific Life, a Fortune 500 Company, is one of the largest financial institutions in the US. Founded in 1868, they offer a wide range of products and services, including life insurance, mutual funds, annuities and other investment products for individuals and businesses. More than half of the 100 largest companies in the US are Pacific Life customers.

A STORY OF CLOUD ADOPTION

In 2013, the Retirement Solutions Division at Pacific Life began planning the migration of a portion of their workload to the public cloud. Reza Salari, Manager of Information Security and Telemetry, drove the cloud migration effort. Until that point, Reza's small team of only three engineers used an array of tools to manage their cross-country VMware® data centers. In moving to the public cloud, they sought to optimize operations without increasing their team size. After exploring public cloud options, the team chose Amazon Web Services (AWS), for its business differentiating value.

The first workload they moved to the cloud was their actuarial grid computing which included resource-depleting hedging models. Today, four years later, the team has approximately 100 EC2 instances that run regularly; however, when running a hedging model, this number can increase significantly for a short time. With Amazon EC2 spot instances, they are able to deal with this elastic demand by bursting to 2,000 instances while running a cost efficient cloud footprint. In addition to EC2 instances, the team also uses RDS for databases, S3 for their object storage, and Glacier for archiving.

Compliance and regulations are major areas of concern in the insurance industry. Reza and his team are responsible for adhering to national regulations like Sarbanes Oxley as well as regional requirements such as the New York Financial Responsibility Laws. In an effort to manage all their layers securely and at scale, the team has employed a mix of AWS security products, including CloudTrail, KMS, and third party tools such as Splunk for log analytics, and **CloudGuard Dome9** for cloud infrastructure security management.

THE DRIVE FOR NEW SOLUTIONS

Need 1: Manage Network Security

Pacific Life's AWS network includesover 150 security groups across seven Amazon cloud accounts in three US regions, with each varying between 5-20 security rules. In total, their network deployment holds thousands of rules in a constantly changing elastic cloud environment. A system issue compelled Reza's team to understand that moving forward, they wouldn't be able to control the growing complexity with AWS native tools as they expanded their footprint and would need to make some changes. This included building new networks leveraging both AWS, VPCs and even nested security groups (security groups that reside within other groups).

Solution: Active Protection and Enforcement with CloudGuard Dome9

CloudGuard Dome9 allows businesses to actively assess, remediate, and control the state of their network at all times. The platform helps Reza's team easily manage security and compliance across their entire Amazon environment. With CloudGuard Dome9, Reza's team can continuously monitor their VPCs and security groups, and the system will provide real-time alerts in cases of misconfigurations, such as an open IP port. In addition, the team relies on the system to stop unauthorized users from modifying security groups and automatically reverts unintended or malicious policy configurations. For example, if a user changes a security group policy to allow inbound SSH traffic, CloudGuard Dome9 can detect this change, revert it, and alert the team.

Separation of Duties

Other teams, such as the DevOps team, occasionaly needed to reconfigure settings; while the compliance team needed to review and ensure the security prior to deployment. Before implementing CloudGuard Dome9, Reza's team was challenged with providing access to the other teams while maintaining control and ensuring that they were the only ones with access to configure the network security. This resulted in a cumbersome, manual, error-prone process. Today, with consolidated control over all the AWS accounts created by CloudGuard Dome9, Reza's team can easily set up access for these other teams to specific subnets and infrastructure elements. The CloudGuard Dome9 service allows Reza's team to enforce and monitor separation of duties more effectively than before. If anyone attempts to change a configuration outside of the defined policies, CloudGuard Dome9 will simply revert back to the correct settings, ensuring control. As Reza puts it, so that "There is only one chef in the kitchen."

Immediate Remediation

Policy misconfigurations in the public cloud can expose the network to outside threats. CloudGuard Dome9 detects these misconfigurations and immediately alerts the security operations team via an SMS message to their mobile devices. The message includes the cause and a corresponding action path to fix the issue and return the system to optimal operation. Receiving the alerts in real-time allows the team to quickly remediate vulnerabilities and prevent security issues.

Visualizing VPC Flow Logs

With the introduction of AWS VPC Flow Logs back in 2015, the team decided to leverage the capability to learn about traffic flows and troubleshoots issues. Once enabled for a particular VPC, relevant network traffic is logged to Amazon CloudWatch Logs for storage. However, it was difficult for Reza's team to make sense of all the data from these logs, in particular when it came to controlling seven different AWS accounts. The CloudGuard Dome9 platform's powerful visualization tool Clarity, provides a real-time topology of security groups and an intuitive visual representation of VPC Flow Logs. This allowed the Pacific Life team to identify security risks and operational issues, visualize policies and remediate threats on all of their accounts, all from a central console.

Need 2: Accelerate Software Delivery

Prior to CloudGuard Dome9, the R&D and Ops teams lacked a way to quickly test the security posture of software products early in the software development lifecycle (SDLC). More than once, the DevOps team deployed workloads only to find that they were not designed properly from a security and compliance perspective. Reza's team was also looking for ways to accelerate product delivery by leveraging DevOps tools such as AWS CloudFormation, AWS CodeCommit and Chef. Even as the product lifecycle became accelerated, security reviews of new release candidates needed to be streamlined and efficient.

> *"CloudGuard Dome9 is a huge force multiplier, providing tools that are highly effective and efficient. Because CloudGuard Dome9 is enabling our cloud strategy, we can innovate and offer better products, while lowering our expense ratio, giving customers better value."*
>
> **Reza Salari**
> Manager of Information
> Security and Telemetry,
> Retirement Solutions Division
> Pacific Life

Solution: Integrate Security Review to Reinforce Development

The DevOps team at Pacific Life uses **CloudGuard Dome9 Clarity** to understand the security configuration of their applications and how each one must be built. Clarity provides a granular view of cloud assets, including VPCs, security groups, and instances, automatically looking for any misconfigurations. By combining Clarity with AWS Flow Log support, Pacific Life can identify what traffic is being accepted vs. that which is not, and manage adjustments as needed, all from a single pane. They are also able to check their stack before deploying it into production. Once checked by the Dev team, and as it moves into production, Reza's team takes the next step, checking the new deployment to validate its network security. In addition, the team uses the Compliance Engine from CloudGuard Dome9 to continuously run audits against their cloud deployment to make sure the deployment follows their policies and best practices, such as the CIS AWS Foundations Benchmark.

Need 3: Control Data Residency

Compliance and regulations are cornerstones of the insurance industry and therefore keeping information inside the US is critical. For regulatory reasons, Pacific Life cannot have US data being sent out of AWS cloud US regions. Additionaly, as mentioned, Pacific Life's cloud environment spans multiple AWS US regions. In order to comply with regulations, Reza's team had to control and prevent usage of AWS regions outside of the company's approved US regions.

Solution: Locking-out Non US Regions

CloudGuard Dome9 complements the ease of access to AWS and the cloud's great global presence with its security controls, leveraging AWS security building blocks. CloudGuard Dome9's active protection is two fold, and guarantees that no unauthorized network changes will be made to the AWS account, utilizing CloudGuard Dome9 as the security policy definition and enforcement point for all organizational security policies. CloudGuard Dome9's Tamper Protection locks the existing security groups and guarantees that no network changes can be made unless they are created via the CloudGuard Dome9 console. In addition, using CloudGuard Dome9 Region Lock, the team configures policies about how the system automatically treats newly available security groups. CloudGuard Dome9 Tamper Protection and Region Lock ensure secure and consistent security group configurations, making sure that their sensitive data remains compliant, preventing any practical usage of unauthorized AWS regions.

THE BENEFITS OF USING CLOUDGUARD DOME9

Cloud Adoption

CloudGuard Dome9 has given Pacific Life the end-to-end visibility and control needed to run sensitive workloads securely on AWS. Reza and his team have the knowledge-backed confidence to defend their cloud initiative to senior management. Reza states, "CloudGuard Dome9 has given me the confidence to tell senior management that the cloud is safe and open for business. The CloudGuard Dome9's comprehensive and mature security solution allows us to be innovative and take risks we couldn't otherwise. It was and still is a critical element in our cloud journey which eventually helped us save $1.1 million in 2016" said Reza Salari, Manager of Information Security and Telemetry for Pacific Life's Retirement Solutions Division.

Cost and Time Efficiency

Insurance/annuities is a risk averse industry. Yet Pacific Life's changing customer base expects them to be more dynamic, delivering information faster and bringing new products to market quickly. With CloudGuard Dome9, robust security does not get in the way of delivering quality products faster. The CloudGuard Dome9 solution allows security and compliance to be incorporated early and often into the continuous integration/continuous delivery (CI/CD) pipeline. Engineering teams can run security checks at the testing phase rather than at the end, enabling them to find and fix security vulnerabilities early. "CloudGuard Dome9 is a huge force multiplier, providing tools that are highly effective and efficient. Because CloudGuard Dome9 is enabling our cloud strategy, we can innovate and offer better products, while lowering our expense ratio giving customers better value," said Reza.

FINAL NOTE: SECURITY AT SCALES

The whole company is aligned on a ten year roadmap to move to the cloud. As the champion for cloud adoption, Reza plans to have the majority of Pacific Life's specific department assets running on AWS within the next three years and knows that CloudGuard Dome9 will be able to scale just as well as it does now.

Pacific Life's services are used and trusted by milions of people across the US and beyond. CloudGuard Dome9 will continue to play a strategic role when it comes to remaining an agile, relevant and secure player in today's financial sector.

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

CONTACT US
Check Point Software Technologies Ltd.
959 Skyway Road, Suite 300
San Carlos, CA 94070
USA +1-800-429-4391
www.checkpoint.com

For a free security assessment or trial, please contact:
US Sales: +1-866-488-6691
International Sales: +44-203-608-7492

CDPLCS12172018