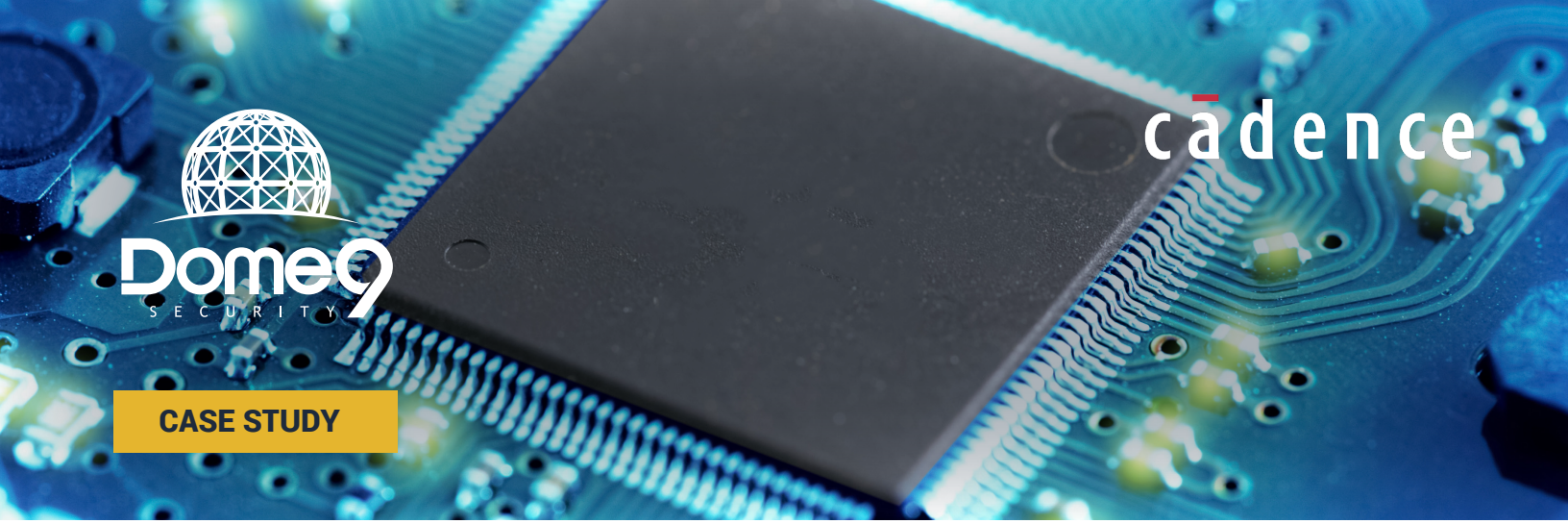

CASE STUDY

"When deploying a multi-cloud environment, you need to have a consistent tool that plays across all the platforms. Using the cloud-agnostic Dome9 Arc platform, I only need to train an individual on one set of tools and he can manage our total cloud environment very effectively."

Sreeni Kancharla
Chief Information Security Officer & Sr. Group Director

CADENCE USES DOME9 ARC FOR ROBUST SECURITY ACROSS ITS MULTI-CLOUD ENVIRONMENT

ABOUT CADENCE

Headquartered in Silicon Valley, Cadence Design Systems, Inc., founded in 1988 is a global technology company that spans 40+ countries with over 8,000 employees worldwide. Cadence supplies electronic design technology and engineering services in electronic design automation (EDA) to much of the semiconductor industry including Fortune 100 companies. Cadence produces software, hardware and silicon structures that are used to design integrated circuits, systems on chips (SoCs) and printed circuit boards.

CADENCE'S JOURNEY TO THE PUBLIC CLOUD

Originally, Cadence ran their own datacenters and found those to be sufficient for their computing needs. However, as the enterprise expanded, it began to outgrow the computing capacity of its on-premise system. Cadence needed a system that has scalability, elasticity and securely enabled cloud demand. Sreeni Kancharla, Chief Information Security Officer (CISO) and Sr. Group Director for Cadence, and his team of ten engineers, including his head Cloud Architect, Koji Kuramatsu, turned to Amazon Web Services (AWS) for help. With the resource capabilities supplied by AWS at their fingertips, Cadence was able to provide the computing power necessary to respond to customers' requirements instantaneously as needed.

Cadence started their public cloud journey in 2014. Today Cadence primarily uses AWS, via 50+ accounts. Cadence has a presence in mainly three of AWS Regions worldwide which include the USA West and East Coasts, and Europe. It makes full use of the AWS cloud functionality for production utilizing services for compute, storage, networking, database, security, developer and management tools. Cadence's AWS footprint covers more than 1,000 instances, 770 security groups, and 115 Amazon VPCs, with more than 4,000 different network security policies and rules, which leaves Kancharla and Kuramatsu with the challenge of securing a very dynamic cloud environment. In addition, while AWS is their primary cloud service, Azure is also represented with tens of compute and storage resources deployed in 29 security groups. They have also begun incorporating Google Cloud Platform (GCP) into their multicloud environment.

CADENCE TACKLES CLOUD CHALLENGES WITH NEW SOLUTIONS

From the get go, Kancharla knew that migrating to the cloud would bring challenges in the realm of network security, compliance and visibility. He needed to be sure that any cloud management integrated solutions would be compatible and effective across the major public cloud infrastructures-as-a-service (IaaS) providers, which included AWS, Azure, and GCP. Due to their anticipation of these security challenges, Cadence began using Dome9 as soon as they moved to the cloud.

Challenge 1: Visibility in a Multi-Cloud Environment

Visibility into the cloud is vital in order to control security and minimize the infrastructure attack surface. With the highly-dynamic nature of the public cloud and unlimited amount of resources it would afford its customers for scalability, the need arose to tightly monitor and track the various network configurations. According to Kancharla, *"With several administrators adding to the cloud configuration, the occasional misconfiguration is inevitable. With thousands of constantly shifting rules across hundreds of security groups and VPCs, Cadence's cloud presence is far too big and complex to be managed by humans. It's impossible for an individual to manage it. We needed an automated tool that actually tracks all the changes."*

When a change occurred, Kancharla's team needed to be able to peer into the system to see exactly what took place so that it could be corrected quickly. Cadence needed to automate repetitive tasks such as security group auditing, fix any misconfigurations with in-place remediation, and have built-in active protection to enforce established policies with the ability to track and revert unwanted changes consistently.

Solution 1: Dome9 Clarity for Granular Network Visualization

Cadence found their solution in **Dome9 Clarity.** As part of the Dome9 Arc platform, Clarity is a powerful visualization capability that provides a granular view of network topology and workflow traffic so Kancharla's team can easily map all subnets and drill down to view reports of all AWS EC2 instances on a single, easy-to-use dashboard. In addition, Cadence uses Dome9 Clarity to check their AWS VPCs state and overall network exposure. This includes using **Dome9 IP Lists** for grouping and configuring permissions to specific public IPs. Using Dome9 Clarity, Cadence has centralized management of its network security posture and can efficiently whitelist those IPs that can be viewed coming to and leaving from their security groups, in order to define the internal and external network links.

One of Cadence's most common uses for Clarity, is to find potential vulnerabilities that would create a security alert. Clarity gives Kuramatsu a quick view of a specific subnet or route going from A to B so he can quickly identify any unauthorized changes to the network. In addition, the **Dome9 VPC Flow Logs** allow the team to quickly respond to events without the efforts of cumbersome investigation of the data logs.

> *"When deploying a multi-cloud environment, you need to have a consistent tool that plays across all the platforms. Using the cloud-agnostic Dome9 Arc platform, I only need to train an individual on one set of tools and he can manage our total cloud environment very effectively."*
>
> ***Sreeni Kancharla***
> *CISO & Sr. Group Director*
> *Cadence*

Challenge 2: Maintain Access Control While Providing User Flexibility

Enforcement of access and authorization to ports and services are vital in a complex cloud network. One of the main concerns Cadence faced was protecting their customers' data while providing multiple users access. Cadence needed a tool that could not only monitor, but protect the movement of resources both between the segregated subnets as well as on and off the

public cloud networks. This tool would ensure that only authorized individuals could access specific data, make changes, and enforce only authorized changes.

At the same time as securing access, Kancharla had the added challenge of retaining flexibility. Cadence provides training sessions for their customers which requires the off-site trainer to enter the Cadence system remotely from the customer's site. However, permitting such ad-hoc temporary entry naturally puts the network at risk and makes it vulnerable to outside threats. Kancharla's team sought a solution which would bring the capability to add access without compromising strong security controls.

Solution 2: Dome9 Active Protection for Security Enforcement

Kancharla recognized that the cloud security solution he implemented needed to offer full security orchestration, going beyond monitoring and reporting to include enforcement. Automated control over the implemented and established baseline security posture was essential. Within the Dome9 Arc platform, Kancharla found the control he was looking for with the always-on security enforcement of Dome9's Active Protection. With active protection, Cadence acquired the following three-pronged approach to the challenge of granting user access and providing flexibility and agility to its customers, while securing their multi-cloud environment with confidence.

• **Dome9 Dynamic Access Leases:** *"We use Dynamic Access Leases heavily*," says Kuramatsu. He and others on his team use Dome9's Dynamic Access Leases to solve the challenge of individuals who need temporary remote access to the network. With Dynamic Access Leases, the person can get specific temporary access to only those parts of the networks that he needs for a limited time frame. The Dome9 tool opens up the ports automatically and closes access again at the end of the defined time frame, thus reverting to the original, defined network state, ensuring consistent protection across their clouds.

• **Dome9 Tamper Protection:** Attempts to modify a security group from the multi-cloud environment will result in Tamper Protection detection and a message. Cadence's pre-defined policy in Dome9 is always enforced, and any modification attempt will be overridden, forcing the policy to revert to its original definition. Kancharla's team leverages this capability to make sure there are no port changes that result in configuration conflicts, especially in the case of network configuration updates.

• **Dome9 Region Lock:** Since Cadence operates across three AWS regions, Kancharla and Kuramatsu rely heavily on Region Lock to enforce regulations which prohibit moving data between regions. Cadence uses Region Lock to ensure that information cannot be moved outside of the USA or Europe. Furthermore, with Region Lock, Cadence can make sure that user access is granted accordingly and employees cannot view data that they should not be seeing. With Region Lock, Cadence can make sure that user access is granted accordingly and employees can not view data that they should not be seeing.

Challenge 3: Compliance Reporting for Customers

Cadence is a large public enterprise that serves leading industry vendors. As such, customer trust is key. With the migration to the cloud, Cadence had to be able to continue to demonstrate consistency with industry standards such as ISO 27001 and other cyber security frameworks' best practices in order to reassure their customers that their applications and data are safe.

Solution 3: Dome9 Compliance Automation and Reporting

The Dome9 Compliance Engine, part of the Dome9 Arc platform, delivers continuous end-to-end compliance testing and reporting against industry standards using automated data aggregation and an intelligent insights generation system. Cadence turned to the Dome9 Compliance Engine to generate compliance reports for AWS and Azure.

Kuramatsu notes that Dome9 best practices reports are, "One of the best parts

of the Dome9 Compliance Engine and we use them quite often." They also use Dome9 to validate their cloud security against CIS AWS Foundations Benchmark framework, which is a set of security configuration best practices to protect one's footprint on AWS. Kuramatsu can prove how robust Cadence compliance truly is by producing compliance reports and quickly respond to Cadence management requests, with well-structured and trusted information.

DOME9 ENABLES LEAN, AGILE, AND EFFECTIVE OPERATIONS

Without Dome9, Cadence would have to spend far more on both the salaries and the training of additional SecOps personnel. Kancharla estimates that Dome9 saves Cadence more than $450,000 annually in not needing to hire an additional three team members enabling his team to run lean. Kancharla states, "When deploying a multi-cloud environment, you need to have a consistent tool that plays across all the platforms. Using the cloud-agnostic Dome9 Arc platform, I only need to train an individual on one set of tools and he can manage our total cloud environment very effectively."

Dome9 Arc provides substantial cost savings by limiting training expenses and enabling Kancharla's team to run leaner, which is a huge benefit as Cadence's cloud environment continues to grow. Dome9 enables Cadence to remain efficient and agile, automating security and compliance management, allowing his team to focus on higher level tasks.

FUTURE PLANS

Cadence is eager to continue evolving and expanding their enterprise so they can provide their customers with the latest engineering design technology within shorter turnaround times. Cadence understands that improving the ability for a customer to innovate and accelerating a customer's time-to-market is imperative. For 2018, Cadence plans to expand its cloud support for Azure, for its customers that rely on Microsoft technologies and are looking to begin their cloud journey. Cadence will continue to use Dome9 to grow securely in the cloud with confidence, knowing they are providing their customers with the most comprehensive and robust security and compliance solution available today.

ABOUT DOME9 SECURITY

Dome9, the public cloud security company, delivers peace of mind to enterprises through security and compliance automation as they scale in any cloud. With Dome9, organizations gain full visibility and control of their security posture, allowing them to minimize their attack surface and protect against vulnerabilities, identity theft, and data loss in the cloud. Dome9's agentless SaaS solution provides operational efficiency for faster time-to-protection. Enterprises choose Dome9 as their key partner to provide the active protection necessary throughout their cloud journey.
Learn more at **https://dome9.com**

CONTACT US
Dome9 Security, Inc.
701 Villa Street
Mountain View, CA 94041 USA
+1–877-959-6889
https://dome9.com
contact@dome9.com

For a free security assessment or trial, please contact:
US Sales: +1-877-959-6889
International Sales: +44-20-3322-3209

DCCS09122018