

DATASTREAM CONNEXION IS BUILDING SECURE FEDERAL AND HEALTHCARE APPLICATIONS WITH CLOUDGUARD DOME9



Customer Profile

DataStream Connexion is a premier technology consulting and web application development agency.

Challenge

- Simplify implementation to limit vulnerabilities and mitigate risks
- Enable strict policies for different security groups, to limit access to sensitive environments Automate and validate compliance status at scale of FedRAMP, NIST and HIPAA for Government and healthcare customers

Solution

- Check Point CloudGuard Dome9
- Check Point CloudGuard Dome9 Clarity
- Check Point CloudGuard Dome9 Continuous Compliance

Results

- Provided powerful security visibility enabling flexibility and insight into real-time network activity
- Allowed easy verification and demonstration of compliance to customers
- Proved, with the right tools, the AWS environment would be the right environment for Federal and Health care sensitive workloads

“We have not had to increase our headcount in moving to the cloud because of the comprehensive and easy network security and compliance CloudGuard Dome9 provides. We are cognizant that if we were still back in the old days, still in colo’s and afraid to make changes, we would not be in the position we are today, providing robust security in protecting the US food chain and building other applications for healthcare and federal agencies.”

—Eric Hoffman, President

Overview

DataStream Connexion

DataStream Connexion is a premier technology consulting and web application development agency. Formed in 2000, they have built web applications for the Federal Government, USDA, FDA, the Department of Homeland Security, healthcare organizations, Fortune 500 companies and small businesses looking for best-of-breed solutions. This small yet nimble team, led by Eric Hoffman, President and owner, provides services that range from product development and DevOps, to cloud security and compliance. DataStream Connexion excels at incorporating comprehensive security and compliance management into the innovative products they design, and thus have garnered the trust of many government agencies and healthcare organizations with maintaining their critical applications in the cloud.



Background: An Early Cloud Adopter

In 2006, Amazon opened the door to the cloud with Amazon Web Services (AWS), providing a more robust and resilient infrastructure solution. Seeing great potential, Eric made the strategic decision to migrate both compute and storage to Amazon EC2 and S3 respectively. In addition, as AWS matured, DataStream Connexion's customers benefited from the evolving robust security controls as well as certifications such as FISMA, SAS-70, ISO 27001 and HIPAA that AWS has to offer.

Leveraging AWS Govcloud

With the introduction of AWS GovCloud in the US region in 2011, the team also recognized the great opportunity of the cloud when it came to hosting highly regulated workloads. This newly introduced Amazon GovCloud was a perfect fit for their customers, supporting the common AWS security controls and compliance standards, but in an isolated, dedicated region, designed specifically for sensitive government agency data. However, in the early days of the public cloud, there was still pushback from Datastream Connexion's federal customer base who were unsure of securing their data in AWS.

During this early cloud adoption stage, Hoffman and his cloud operations team knew that the advantages of AWS were many. However, they also understood their part in the AWS shared responsibility model and that it presented a new set of challenges they would have to overcome to make their customers' cloud adoption journey a successful one. They began to search for tools that would help them build out the visibility and compliance their customers depended on, in order to increase their customers' trust in this new Infrastructure as a Service (IaaS) model. It was the same year that Hoffman found CloudGuard Dome9 and they became one of CloudGuard Dome9's earliest adopters. Since then, as Hoffman states, "CloudGuard Dome9 has become our trusted partner in ensuring the security posture of all DataStream Connexion customers."

Business Challenges

Navigating the Network Security Challenge

As with every new technology adoption scenario, there were challenges that had to be worked out along the way. With the CloudGuard Dome9 platform by their side, DataStream Connexion was able to address and mitigate each one of the following challenges.

Challenge 1: Effective and Efficient Security Management

DataStream Connexion has tens of VPCs and security groups, which end up creating an elastic cloud environment consisting of hundreds of inbound and outbound rules.



“CloudGuard Dome9 has become our trusted partner in ensuring the security posture of all DataStream Connexion customers.”

—Eric Hoffman, President

They also have temporary rules that come and go as their Dev and Ops teams provision temporary access from different locations to allow their flexibility. The first priority was to simplify governance and policy implementation, to limit vulnerabilities and mitigate risk.

Challenge 2: Providing Access While Ensuring Integrity

DataStream Connexion’s small yet agile team of developers, database admins, network admins and generalized office staff all have different needs within AWS. The Ops team has to be able to provide access to various resources for development and specific environments for production, while enforcing strict segregation according to predefined user roles. This means running strict access policies for different security groups in order to avoid widespread administrative access to sensitive highly regulated environments.

Challenge 3: Allow The Broader Team Self-servicing and Flexibility

One facet separating DataStream Connexion from their peers is a bond of trust and accountability among the entire staff, including Ops, Dev and Test. The team practices continuous integration/continuous deployment (CI/CD) DevOps methodologies to move rapidly, without being bogged down with cumbersome legacy procedures that can hinder progress and agility.

This means allowing individuals remote access to their cloud environment at anytime. However, providing remote access requires a change in network security rules, which includes security ports. This is a potential landmine, as enabling the broader team to change configurations is clearly prone to human errors.

Challenge 3: Allow The Broader Team Self-servicing and Flexibility

One facet separating DataStream Connexion from their peers is a bond of trust and accountability among the entire staff, including Ops, Dev and Test. The team practices continuous integration/continuous deployment (CI/CD) DevOps methodologies to move rapidly, without being bogged down with cumbersome legacy procedures that can hinder progress and agility.

This means allowing individuals remote access to their cloud environment at anytime. However, providing remote access requires a change in network security rules, which includes security ports. This is a potential landmine, as enabling the broader team to change configurations is clearly prone to human errors.



Challenge 4: Implementing End-to-End Compliance Management

Adhering to compliance standards can be complex. This is especially true for DataStream Connexion, whose customer base is made up of federal agencies which must adhere to standards such as FedRAMP and NIST. In addition, over the last year, AWS has expanded its offering for the healthcare market, and Datastream Connexion's customer base has also grown in this segment with the customers' focus on HIPAA compliance. Tracking compliance status is no small feat, and a complex cloud network must be consistent and reliable when it comes to different rules posed by various regulatory compliance standards requirements. When it came to validating compliance at scale, Hoffman realized that running manual checks was not an option and would eat up much of his team's valuable time and resources.

Solution 1: Complete Visibility Over the Entire Infrastructure

Network security with CloudGuard Dome9 Clarity allows the team to visualize their cloud perimeter, network topology, security policies and configurations in real-time. It lets them see how the network changes, including configurations of different security groups, as well as being able to drill down to see each instance exposure and its security group assignment. CloudGuard Dome9 Clarity allowed them to quickly spot misconfigurations and eliminate vulnerabilities such as open ports or broken network links between different system tiers. Finally, CloudGuard Dome9 Clarity eased policy analysis, helping the team to enhance rules and strengthen their network security policies with quick links to edit relevant rules and components.

Solution 2: Implementing RBAC to Allow Work to Flow Unhindered

As mentioned above, together with CloudGuard Dome9 Clarity and CloudGuard Dome9's role-based access control (RBAC) capabilities, all Dev and Ops members have access, but only the team admin is able to adjust settings – such as opening user restrictions to a specific security group. The Ops team is able to provide developers the instant access they need to test out new processes, which helps them accomplish their goals faster and with greater ease.

While it is very important for Hoffman to trust his staff and allow them to be nimble and empowered to do their work, if a change has been generated, it is critical that he can oversee it to ensure that it has been implemented properly. CloudGuard Dome9 Alerts keep him aware of what is taking place at all times, and he can always inquire about events as needed. This allows for fast paced innovation, enabling flexible access to the different environments without compromising their network security posture.



Solution 3: Controlled Temporary Access

CloudGuard Dome9 Dynamic Access Leases allow DataStream Connexion to schedule time-limited and on-demand access to services and ports, so that when the time allotted has ended, all ports are closed by default. Access is provided on an as-needed basis, reducing open port exposure, even via mobile device or with the Chrome Browser extension. With CloudGuard Dome9 Tamper Protection, the environment is continuously monitored for any changes to the last approved state. All changes are reverted back automatically, and the Ops team is immediately alerted to validate the policy change. Finally, the risk of open port exposure is dramatically reduced, and the DataStream Connexion staff has the access they need at the click of a button.

Solution 4: Automating Compliance with the Compliance Engine from CloudGuard Dome9

One of Hoffman's most important weekly tasks is reviewing the Compliance Engine's policy reports from CloudGuard Dome9. This comprehensive compliance and governance solution simplifies complicated procedures with automated data aggregation in real-time, and in-place remediation control which streamlines the analysis process, saving hours of complex work. The team can create and enforce custom policies unique to DataStream Connexion's needs, while identifying risks and gaps using built-in test suites for common compliance standards such as HIPAA. In addition, the Compliance Engine from CloudGuard Dome9 continuously runs audits against their cloud deployment, and with it the team can validate its network security posture as well as report the current exposure status and vulnerabilities across their whole cloud network. Leveraging the easy to use dashboards and controls, the team benefits from this transparency and can enforce their established policies and be confident in their cloud compliance status at any point in time.

Results

A Secured Network

The CloudGuard Dome9 service plays a critical role in helping DataStream Connexion mitigate the security challenges of a cloud-based environment. With it, Hoffman's team has complete visibility into all configurations, holes, inconsistencies, vulnerabilities and any setting that has been modified. Hoffman states: "I want my staff to be nimble and empowered to do their work, where I can trust them to keep moving forward. I have the ability at any time, in real-time, to assess why a port may be open. CloudGuard Dome9's logs and alerts are really important to me and enable my employees to be agile and work in the fashion they need to."

The most valuable aspect of CloudGuard Dome9 to Eric is the network security visibility and transparency it provides. CloudGuard Dome9 Clarity lets his team work unhindered while he can see and understand what is going on, day-to-day, minute-to-minute. With CloudGuard Dome9, he is able to give his developers the autonomy they need to work rapidly, without ever taking his eyes off what is happening behind the scenes.



Proven Cloud Compliance

The Compliance Engine from CloudGuard Dome9 has proven to be an effective sales tool, as it allows Eric's team to easily verify compliance to customers with one click, showing how their cloud environments are in line with the strict federal and healthcare regulatory compliance standards. According to Hoffman, "People come to Datastream Connexion because we are known for our robust security. CloudGuard Dome9 provides us with a clear way to demonstrate that."

He notes that there were occasions where government agencies brought his team applications that had been developed by other independent software vendors. When it became apparent that their services were falling short in terms of security, they were handed over to the Datastream Connexion team. With the help of CloudGuard Dome9, the team quickly and seamlessly enhanced the security of the applications, winning the confidence and future business of these government agencies.

Future Plans

Leveraging their existing customer relationships and confidence, Hoffman's team was able to prove that equipped with the right toolset and skills, the AWS cloud would be a great fit for his customers' sensitive federal workloads.

With their expansion on the horizon, Eric Hoffman is fully confident that Datastream Connexion can handle the challenges that come with growth. With CloudGuard Dome9 protecting their infrastructure, they are enthusiastic about where their journey will take them.



For more information, visit:
<https://www.checkpoint.com/products/>