CASE STUDY

Dental Support Services Company Prioritizes Cloud Security

McAfee® MVISION Cloud supports rapid expansion, digital transformation, and compliance

Pacific Dental Services

Customer Profile
Offloads administrative support for dental practices throughout the United States

Industry
Healthcare

IT Environment
More than 750 offices in 22 states, vast amounts of personal health information (PHI) and personally identifiable information (PII) migrating from on-premises data centers to the cloud

Employees
More than 11,000 employees plus 10,000 team members worldwide

Pacific Dental Services (PDS) was founded in 1994 by Stephen Thorne, supporting its first office in Costa Mesa, California. With the vision to create the greatest dental company in the U.S., PDS has expanded to include more than 750 offices in 22 states and is currently experiencing a quickening growth path. PDS expects to add more than 100 offices per year.

Connect With Us

Hyperscale in the Cloud with AWS

In February of 2018, the executive team at PDS decided to move from legacy electronic medical records (EMR) to a new system provided by leading software provider Epic. This initiative kicked off an entire IT transformation centered around the cloud.

"When we started our data center migration, we quickly realized that buying rack space wasn't going to scale with our business," said PDS Senior IT Security Analyst Maka Guerrero. "Our legacy applications were not going to run parallel with our standards from a security perspective."

With the business experiencing hypergrowth, the IT teams at PDS knew that they needed their data centers to scale at the same pace as their business. PDS decided to leverage the efficiency and speed that the cloud could provide. The organization started by leveraging Amazon Web Services (AWS) to store strategically aligned data sets that correspond with their rapid expansion. Following the best practices outlined in the AWS shared responsibility model, Guerrero and the security team at PDS knew they needed to apply additional security controls to their AWS environment to help prevent misconfigurations that could expose their sensitive data.

"We needed to be able to fully govern our data as we made the move to Epic," says Guerrero. "AWS doesn't care what you put in the cloud… It could be Social Security numbers or a basic set of data… We needed additional tools that would allow us to govern our data while still providing our customers and doctors access to information anywhere and at any time."

With both sensitive personal health information (PHI) and personally identifiable information (PII) from more than 750 dental offices migrating to the cloud, the security team at PDS also faced industry regulatory compliance challenges like the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Trust Alliance (HITRUST). They knew that they needed to have additional security controls and parameters in place as they continued their cloud migration. With this in mind, the team decided to move forward with the selection process for a cloud access security broker (CASB) to help provide contextual and privileged access controls to their data.

The team at PDS chose McAfee MVISION Cloud as their CASB provider because of its seamless application programming interface (API) integration to the cloud services they use and its ability to extend their existing on-premises security to their data in the cloud.

"MVISION Cloud allows us to have more flexibility on the fly than any other CASB on the market," says Guerrero. "The approach that McAfee is taking to secure the cloud aligns really well with our other partners like AWS and what they are trying to achieve, and it makes sense for our business goals."

Challenges

- In a state of hypergrowth, the technology stack needed to scale with the business.
- Vast amounts of sensitive data had to be migrated to the cloud, while meeting strict regulatory compliance with industry standards like HIPAA and HITRUST.
- Owner-doctors in more than 750 offices required uninhibited access to patient records at any time on any device via the Epic migration.

McAfee Solution

- MVISION Cloud for AWS
- MVISION Cloud for Box
- MVISION Cloud for Custom Apps
- MVISION Cloud for Office 365
- MVISION Cloud for Salesforce
- MVISION Cloud for Shadow IT

Leveraging User Behavior Analytics to Secure Sensitive Data

With nearly 90% of all sensitive cloud data residing in either sanctioned Software-as-a-Service (SaaS) or Infrastructure-as-a-Service (IaaS) applications, it was imperative for PDS have a clear understanding of where their potential threats reside. This is why Guerrero and the security team at PDS leveraged MVISION Cloud's machine-driven user entity and behavior analytics (UEBA) capability. Now they can instantly analyze the billions of cloud events that occur daily in their environment and have information to establish a baseline of user behavior.

"What the marketing team or HR team does and has access to is significantly different than what we will see out of our healthcare revenue business operations center that deals with and processes insurance claims," says Guerrero. "MVISION Cloud's user behavior analytics provides us with the data that we need to process behavior by user type and line of business, helping us cut through the noise."

This granular insight helps the teams at PDS identify anomalous activity that may be indicative of an insider threat, such as a large upload or download of data or to detect an activity that may indicate a compromised account, such as an impossible -multiple-region access attempt across various cloud services. This type of activity is commonly known as a "superhuman" anomaly and refer to actors attempting to access data across multiple global regions, which is impossible to achieve in a short timeframe.

"The ability to detect and track superhuman anomalies is an important security use case," points out Guerrero. "McAfee delivers on this flawlessly and with a higher efficacy rating than any other CASB on the market."

Additionally, PDS uses MVISION Cloud with a business enablement approach by providing feature sets tailored to the application owners and DevOps teams, including different dashboard views for different teams. This allows them to quickly slice and dice resources across account and region and provides them with relevant, actionable information.

Extending DLP to the Cloud in SaaS Applications, Microsoft Office 365, and Box

Guerrero and his team are taking a platform approach to securing their sensitive data across their entire enterprise. With MVISION Cloud, PDS can extend their existing, on-premises data loss prevention (DLP) policies to their data in AWS S3 buckets—as well as to their sanctioned SaaS applications, such as Office 365 and Box—and apply a standardized set of contextual access controls.

"It is important to PDS to be able to offer cloud-based applications like Office 365 and Box to our customers and have the right security parameters in place so we can successfully protect our data," says Guerrero. "With sanctioned customer-facing tools in place at PDS, it is essential to the business that the owner-doctors can share and collaborate securely with aligned business partners."

Results

- Contextual access controls enable the business to move to the cloud quickly and securely while meeting regulatory compliance.
- DevOps and the information security teams have had their requirements met for real-time, actionable information on insider threats and malicious actors.
- Seamless API integration has reduced friction between security and owner-doctors, increasing sanctioned cloud service adoption and minimizing overall risk

Thanks to MVISION Cloud, the security team has the granular and contextual collaboration controls to prevent sensitive data from leaving unsanctioned cloud services like SharePoint and OneDrive—based on user type, device, and location in real time. MVISION Cloud also gives them with the tools they need to be able to see who did what, when, and where. This provides the security and DevOps teams with real-time activity monitoring on more than 1,600 activities within their environment. This additional insight has provided Guerrero and the team at PDS the opportunity to use just-in-time coaching methods to help change user behavior.

"We believe that patients pay our salaries here," says Guerrero. "We take the initiative in our culture to collaborate like a family, and, sometimes, you just have to be an extra set of eyes on things so you can teach them and say, 'We think this is sensitive data, do you agree?'"

This approach has led to users being receptive to the additional security PDS has put in place which has helped improve their overall risk posture.

"Thanks to the information MVISION Cloud provides us, we can identify our risk and inform the business to determine if they accept that risk," says Guerrero. "We have been able to enhance our overall security posture."

A Cloud-First Enterprise by 2021

"At the end of the day, PDS is a platform and a foundation for dentists to focus on dentistry," says Guerrero. "They don't give you a business minor when you come out of dental school. We allow dentists to do what they do best, and we handle the rest."

With a set of core values that drive their initiatives and put the owner-doctor first, PDS is on its way to becoming a cloud-first enterprise.

"We have a pretty mature mindset when it comes to security, and we would like to be 80/20 with a revised and evolved disaster recovery plan implemented by 2020," says Guerrero, referencing a technology stack that is comprised of 80% of their applications living in the cloud and 20% remaining on premises.

With established security priorities and a foundation of a trusting relationship with its partners and owner-doctors, Guerrero sees great things in the organization's future.

"We have the technical expertise to take that leap and make it work. 2021 will be beyond belief," he affirms.

> "MVISION Cloud allows us to have more flexibility on the fly than any other CASB on the market. The approach that McAfee is taking to secure the cloud aligns really well with our other partners like AWS and what they are trying to achieve, and it makes sense for our business goals."
>
> —Maka Guerrero, Senior IT Security Analyst, Pacific Dental Services

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com