DealerSocket Protects Sensitive Customer Data in Hybrid Cloud Environment

Website
www.dealersocket.com

Region
United States, International locations

Industry
Automotive

Employees
1,000+

Products
Deep Security

IT Environment
Hybrid cloud, Amazon Web Services (AWS), VMware data centers, containers

Business Benefits

- Protects AWS and data center environments
- Helps ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) and other regulations
- Provides robust security for an expanding DevOps practice

OVERVIEW

DealerSocket is a leading provider of software solutions for the automotive industry, offering a suite of seamlessly integrated products to help dealers sell and service vehicles more profitably. Since 2001, more than 100 million vehicles have been sold through the company's software platforms. DealerSocket's software-as-a-service (SaaS) products include advanced customer relationship management (CRM), digital marketing and websites, vehicle inventory management, analytics reporting, dealer management systems for independent dealers, and solutions that streamline dealer operations.

Based in Dallas, Texas, DealerSocket also has offices throughout the U.S. and internationally. The company employs more than 1,000 team members, serving 300,000 active users at more than 9,000 dealerships. DealerSocket's hybrid cloud environment combines Amazon Web Services (AWS) and VMware® data centers. The organization also uses containers for its growing DevOps practice.

CHALLENGES

DealerSocket's top priority is protecting the credit data for more than 100 million auto sales for its customers. The company's IT security team must protect this information on AWS and in its data centers to maintain compliance with regulations in the U.S. and worldwide. The effort was complicated by the acquisition of several new companies, which introduced a variety of tools into the mix.

"We needed to consolidate our security tools on a platform that was scalable, easy to deploy and use, as well as protect our cloud and virtual environments," said Greg Tatum, director of DealerSocket's network and security operations.

In addition to the need for broader and stronger security, DealerSocket wanted a solution that would support its DevOps operation. "DevOps presents unique security challenges," said Tatum. "The move to DevOps requires security tools that our engineers and infrastructure teams can easily embed in applications, in real time as they are built."

"With a trusted partner like Trend Micro and its leadership in Gartner's Magic Quadrant, our customers know their data is protected by one of the best players in the business."

Greg Tatum,
Director of Network and Security Operations,
DealerSocket

"We needed to consolidate our security tools on a platform that was scalable, easy to deploy and use, as well as protect our cloud and virtual environments,"

Greg Tatum,
Director of Network and Security Operations,
DealerSockettt

WHY TREND MICRO

When DealerSocket began its search for a new security solution, they wanted comprehensive reporting capabilities to support compliance with the Payment Card Industry Data Security Standard (PCI DSS) and other regulations. The solution had to be application programming interface (API)-driven, scalable, and easy to manage, install, and use. Finally, the solution would have to work seamlessly across Linux®, Microsoft® Windows®, Mac®, and virtual platforms.

Based on the results of the proof of concept, and on its reputation for innovative and effective solutions, Trend Micro was chosen among three vendors to provide the company's security solution. "With a trusted partner like Trend Micro and its leadership in Gartner's Magic Quadrant, our customers know their data is protected by one of the best companies in the business," said Tatum.

SOLUTIONS

DealerSocket selected Trend Micro™ Deep Security™ to use across all of its hosted infrastructure, including every endpoint within the AWS environment and in the data centers. "Deep Security is required as part of our security policy," said Tatum. "A machine won't go into the field unless Deep Security is installed."

DealerSocket uses Deep Security's antivirus, file integrity monitoring, and network intrusion detection and prevention features to protect its environment and support compliance. The solution's reporting capabilities are instrumental in keeping the company secure across its entire infrastructure. "In addition to daily reviews, Deep Security reports are shared once a month with other teams that support our IT environments as part of our vulnerability and threat management review," said Tatum.

RESULTS

With Deep Security protecting its AWS and data center environments, DealerSocket's security team can quickly detect incidents and efficiently manage investigations, allowing them to provide vastly improved protection for the company's data.

Deep Security also met DealerSocket's ease-of-use requirements from the start. In just 30 days, the solution was easily installed on 2,000 machines and the previous product was removed. The product supports DealerSocket's DevOps goals with its full API enablement and scalability. Finally, Deep Security's tools and reports have significantly simplified its compliance requirements. For example, the company's last PCI DSS audit took only two and a half weeks.

WHAT'S NEXT?

Looking ahead, DealerSocket plans to continue expanding its DevOps practice. Trend Micro is working with Tatum and his team to secure containers and is currently testing container security in its AWS environment. "At DealerSocket, DevOps starts with engineering, infrastructure, and security leadership. We meet weekly to discuss the cultural changes required to make DevOps and security part of our culture," said Tatum.

MORE INFORMATION

For more information, please go to
www.trendmicro.com

TREND MICRO™

Securing Your Connected World