Allegiant Travel Company

Securing traveler information with OpenText Security solutions helps revenues take off.

Overview

Founded in 1997, Las Vegas-based Allegiant Travel Company operates a low-cost, all-jet passenger airline through its subsidiary, Allegiant Air. The company is an industry disruptor: instead of competing directly with big airlines, Allegiant found an interesting niche, targeting leisure travelers with direct flights to over 100 destinations across the U.S.

Challenge

A leader in unbundled travel, Allegiant also competes by keeping its airfares low. To drive incremental revenue, it charges fees for unbundled services such as checked luggage and hotel reservations. The company characterizes itself as more of an e-commerce company than an airline, because 94% of its revenue comes through the website.

> "We would've spent months of developer time bringing legacy systems in to strict PCI compliance. Instead, those developers were allowed to work on projects that are actually revenue-generating."
>
> **Chris Gullett**
> Director of Information Assurance
> Allegiant Travel Company

Leisure flyers looking for deals flock to Allegiant, and the airline must flawlessly process credit card transactions through its website and mobile apps, and protect customer data in the process.

To succeed, Allegiant must deliver a seamless experience to online shoppers looking for vacation deals. If those travelers lose trust in the security of Allegiant's credit card processing, its revenue and reputation are at risk. To protect credit card data and customer information—and comply with the Payment Card Industry Data Security Standard (PCI DSS)—Allegiant needed to apply security measures directly to the data from the point customers engage with the company on its website and throughout the process of booking travel services. As Susan Hulings, VP of Internal Audits, Allegiant Travel Company, explains: "PCI compliance is important. It's really about protecting the customers and their credit card information."

Solution

Allegiant partnered with the OpenText™ Data Security Professional Services team to deploy Voltage by OpenText with Secure Stateless Tokenization by OpenText and Voltage SecureData Enterprise Web by OpenText with Page-Integrated Encryption (PIE).

At a Glance

Industry

Hospitality and Travel

Location

Nevada, USA

Challenge

Protect credit card data and customer information while complying with the Payment Card Industry Data Security Standard (PCI DSS)

Products and Services

Voltage SecureData Enterprise
Voltage SecureData Web
Secure Stateless Tokenization

Success Highlights

- Fast implementation led to enhanced revenues by redeploying development staff to revenue-generating projects
- 100 percent of customer transactions now protected by Voltage SecureData
- No credit card details stored

Connect with Us
www.opentext.com

With this information security and data protection solution, Allegiant encrypts each customer's credit card number the instant it's entered in the browser window on the company's website. That encryption is maintained as credit card data is processed throughout booking. And with Voltage Secure Stateless Tokenization, credit card data is no longer stored in Allegiant IT systems. This has vastly reduced the "attack surface" of systems and applications containing live credit card data.

Taking systems out of audit scope also simplifies PCI compliance and streamlines audits. As a result of this data protection solution, Allegiant achieved compliance without having to deploy developer resources to retrofit the company's legacy software systems. These resources were able to instead focus on value-add and revenue-generating new development. Chris Gullett, Director of Information Assurance, Allegiant Travel Company, comments: "We would've spent months of developer time bringing legacy systems in to strict PCI compliance. Instead, those developers were allowed to work on projects that are actually revenue-generating."

Voltage SecureData Enterprise with Voltage Secure Stateless Tokenization (SST) and Voltage SecureData Enterprise for Web with Page-Integrated Encryption (PIE) enable Allegiant to stand up secure servers in data centers anywhere across geographically dispersed areas, with no need to build and connect separate database infrastructures for key management.

With this capability, the company can easily scale the information security solution with no additional administrative overhead. The Voltage SecureData Enterprise solution also provides a flexible foundation for Allegiant to deploy additional Security solutions to expand encryption to mobile devices and protect other forms of data such as passport numbers and social security numbers.

Results

By implementing the OpenText powerful cyber security and data protection solution, Allegiant is delivering a seamless, secure travel booking experience. Customers are better protected against unauthorized exposure of credit card data, helping ensure fun, worry-free travel. That peace of mind is a boon to satisfaction and loyalty, which elevates Allegiant's brand.

The solution has delivered top-line benefits, too. By freeing product development staff to focus on revenue-generating projects, Allegiant introduced a new application that produced significant additional revenue. For internal operations, the solution has reduced the cost and complexity of the company's PCI audit and compliance processes.

Allegiant has removed credit card data from their payments ecosystem, significantly reducing the scope of IT systems required to achieve compliance with PCI DSS, thus swiftly passing their PCI Level 1 audits and reducing costs.

Maury Gallagher, Jr., CEO and Chairman, Allegiant Travel Company, concludes: "IT equals innovation, pure and simple. We are an IT company that happens to fly airplanes. The ability to control the software and the IT piece is something that makes us better."

opentext | Cybersecurity