



CASE STUDY

Park 'n' Fly: Parkeon Steers Its Applications to a Secure Spot

THE COMPANY | Parkeon is a key global player in the urban mobility market.

QUICK STATS

- Worldwide leader in payment & ticketing solutions for parking, mass transit
- €176 million in revenues (2008)
- Product implementation in 3,000 cities
- Operations in more than 40 countries
- Processes 550,000 payment transactions per month
- Centrally monitors 21,000 terminals per month
- Maintains more than 150 software systems

Case Background

Parkeon (www.Parkeon.com) is one of the world's largest parking and transport management solution providers. Headquartered in France, the company has operations in 40 countries, including the U.K., U.S., Australia, Belgium, Germany, Italy and Spain. Its unique range of services and solutions, together with its constant ability to innovate over the last 35 years, has made Parkeon a unique player within its market. To date, it has developed over 150 software systems and processes 550,000 payment transactions per month while centrally monitoring 21,000 terminals.

Parkeon provides end-to-end electronic payment solutions from transaction processing at the point-of-sale (POS) through to vendor payment by their customers' financial institutions. Parkeon's offerings are complemented by a full range of payment methods including credit and debit cards, mobile phone account, and prepaid cards. These solutions are deployed on Parkeon's own POS terminals, such as parking meters at curbside and at 'pay and display' and 'pay on foot' car parks.

Secure Payment Processing Integral to Parkeon

As a payment processor, Parkeon is very concerned about payment security. A recent study by U.S. mobile network provider Verizon, its annual *Data Breach Investigation Report*, showed that 285 million records were compromised during 2008, which was a major increase compared to 230 million the previous four years. These figures provided the motivation for Parkeon to raise its

KEY CHALLENGES

- Defend parking machines from hackers
- Closely monitor payment systems to ensure a proven level of security
- Maintain the confidentiality of each user's personal data
- Develop application security early in the software development life cycle
- Ensure the system passes the stringent requirements expected by the latest PCI-DSS and PA-DSS standards

application security level system-wide, regardless of the diversity of its customers' geographic locations or the lack of adoption of payment security standards within some countries in which Parkeon operates.

Luc Porchon, banking applications project manager of Parkeon, explains further, "Parkeon has clients all around the world who currently use our products to make and receive payments. The security of these electronic transactions is of paramount importance to us, and therefore we closely monitor our payment systems to ensure a proven level of security. Our payment processing validates the integrity while maintaining the confidentiality of each user's personal data."

Parkeon Subject to PCI Security Standards

To protect the flow of sensitive customer data, the major global credit card issuers have come together in the Payment Card Industry Security Standards Council (PCI-SSC), an open and global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for card account data protection. Its mission is to enhance payment account data security by driving education and awareness of the PCI Data Security Standard, or PCI-DSS for short.

PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. PA-DSS is the program to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data. PCI-DSS compliance is an industry-driven, not government regulatory, mandate. Only payment applications that are sold, distributed or licensed are subject to the PA-DSS requirements. In-house payment applications developed but

not resold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI-DSS.

As Parkeon provides a complete payment solution, it is subject to both PA-DSS and PCI-DSS certification of its software architecture.

Cutting Edge Technology – Guaranteed Flawless

When designing its latest state-of-the-art electronic ticketing and transaction product, *ArchiPEL*, Parkeon knew it was essential that in the very early stages its developers built stringent and secure software with flawless watertight code free of known vulnerabilities to prevent hacking incidents or breaches.

"Security should not be seen as the icing on the cake, being added at the last minute to make an application attractive, but instead as the basic vital ingredient needed to ensure the success of the recipe and therefore incorporated right at the beginning," Mr. Porchon says. "Fortify's expertise was engaged in May 2009, very early on in our development process. They were the natural choice being the application security and testing provider chosen by the U.S. government, the U.S. armed forces, many of the major banks such as ABN-AMBRO and JP Morgan, and numerous Fortune 500 companies."

Fortify products protect companies from today's greatest security risk: the software applications that run their businesses. Any organization storing or processing credit card information must comply with the PCI-DSS or face the risk of losing card processing privileges with the major issuing brands. Specifically, Fortify Software focuses on helping customers pass compliance audits of Section 6 of the standard, the critical set of requirements dealing directly with application security.

Fortify® 360 Secure Your Software

Fortify 360 is a suite of integrated solutions for identifying, prioritizing and fixing security vulnerabilities in software and managing the business of ensuring application security.

Parkeon selected Fortify 360 which enables an organization to conduct static analysis of an application's source code, dynamic analysis of a running application, and real-time monitoring and protection for a deployed application. No other vendor offers all three of these solutions in one integrated platform. For a company such as Parkeon trying to pass PCI-DSS compliance, Fortify offers dynamic security tests, code reviews, and an application layer firewall. Fortify's application security experts are at the cutting edge of software vulnerability research, tool development, and deployment practices.

Parkeon selected Fortify as its primary application security partner based on its ability to reduce risk employing analysis and remediation solutions that can:

1. **Specify the vulnerabilities** within the software so the development organization can eliminate them prior to deploying the application into production.
2. **Implement a continuous review** by testing and verifying the code for security vulnerabilities introduced during development. Mr. Porchon notes, "The specialists at Fortify helped us establish development best practices based on the analysis of our architecture and code base. Then we set up the production environment and ongoing verification processes."
3. **Incorporate security** into Parkeon's preferred integrated development environment.
4. **Build in security gates** to prevent applications with vulnerabilities from ever going into production. This requires finding and addressing vulnerabilities, as they are located.
5. **Track metrics** to gauge the success of the security plan so that the organization can continually improve the process.

For three months, Fortify provided professional services to Parkeon to ensure its success with Fortify 360, checking and scrutinizing its *ArchiPEL* software to ensure that it passed the stringent requirements expected from the latest PCI-DSS and PA-DSS standards. Fortify 360 SCA quickly and easily checked all source code, testing and revealing critical, potentially hazardous vulnerabilities. Fortify trained Parkeon's development team to prioritize their work and helped to seal those vulnerabilities that hackers most commonly target.

"Using Fortify's expertise to test our software at the code development stage and again at various stages in its deployment, we uncovered flaws and then successfully removed them. This partnership has been essential in getting our product to market on time while ensuring it meets stringent compliance standards such as PCI-DSS and PA-DSS," summarized Mr. Porchon. "Fortify has helped us to establish secure development best practices based on its analysis of our software security architecture and application code, and we will continue to use Fortify software to test all our software throughout its life cycle to make ensure it is secure at all times."

Parkeon is on target to move quickly through the next PCI-DSS audit process which will test that their latest innovative and cutting edge payment systems are secure for the customers waiting to use them. In partnership with Fortify, Mr. Porchon remains confident that future secure payment applications will go to market on time and on budget.

Mr. Porchon believes that managing software security risk is a cost of doing business. "A quick estimate of the costs incurred by one instance of compromised data, coupled with the interests of an attacker, provides a sobering quantification of risk. Indeed, the risk is mainly financial, including repair to a compromised image or brand plus any penalties imposed by the PCI CSC offending bank plus any recovery of damages to other players such as the carrier and issuing banks."

FORTIFY BENEFITS

- **Finds and assesses** potential vulnerabilities during Parkeon's software development processes
- **Fosters** an awareness of security risks and the need for remediation by educating Parkeon developers
- **Supports** creation of new security features and continuous methods of locating vulnerabilities in Parkeon's production applications
- **Makes** application security an integral part of Parkeon's IT operations
- **Secures** all applications throughout the entire software development life cycle.
- **Delivers Cost Savings** to Parkeon by finding vulnerabilities earlier

The logo features the number '360' in a large, light grey font, with the word 'FORTIFY' in a smaller, bold, light grey font centered below it. The background is a dark grey with faint, curved lines.

About Parkeon

Parkeon is a leading player in the field of urban mobility. Thanks to its unique transversal offer in terms of parking and urban transportation payment solutions and to its constant ability to innovate, as shown over its 35 years of experience. A leader in payment and ticketing solutions for parking and urban transport, Parkeon provides integrated parking and transport management solutions for local authorities and private operators.

About Fortify Software, Inc.

Fortify®'s Software Security Assurance products and services protect companies from the threats posed by security vulnerabilities in business-critical software applications. Its software security suite—Fortify 360—drives down costs and security risks by automating key processes of developing and deploying secure applications. Fortify Software's customers include government agencies and FORTUNE 500 companies in a wide variety of industries, such as financial services, healthcare, e-commerce, telecommunications, publishing, insurance, systems integration and information management. The company is backed by world-class teams of software security experts and partners. More information is available at www.fortify.com or visit our blog.



FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT WWW.FORTIFY.COM

2215 BRIDGEPOINTE PKWY.
SUITE 400
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600
FAX: (650) 358-4600
EMAIL: CONTACT@FORTIFY.COM