Customer Success Story

The Company
As Europe’s leading independent online travel and leisure group, the company’s websites provide customers in 14 countries with access to airline tickets, hotel rooms, holidays, car hire, entertainment tickets, restaurant reservations gifts and auctions. The company also owns and operates a variety of online brands including a German language site, a car rental site, and a brand dedicated to action-packed adventures.

The Challenge
While the business serves as the online gateway to fun and adventure for millions of customers worldwide, there’s one thing the company doesn’t take lightly: information security. In fact, each of the company’s global websites promises its customers that “any data you transfer through our sites will be completely safe from prying eyes.” The chief architect and security officer for the organization is responsible for ensuring that the company can stand by this promise.

Like all credit card merchants, the organization is required to ensure and validate the security of its network under the Payment Card Industry (PCI) Data Security Standard supported by all major credit card issuers. Under the PCI Standard, the company is required to implement data security measures that include penetration testing. Specifically, Requirement 11.3 calls for network penetration testing to be performed “on network infrastructure and applications at least once a year and after any significant infrastructure or application upgrade or modification (e.g., operating system upgrade, sub-network added to the environment, web server added to the environment)…”

The Solution
To protect the organization’s customer information while complying with the PCI standard, the security officer and his team traditionally performed internal security evaluations using an open source penetration testing solution and a complement of vulnerability scanners. However, as the company expanded its infrastructure to support the growth of its websites, they found it increasingly difficult to pinpoint demonstrable security threats using their existing in-house tools. While external consultants could help to pick up where these tools left off, the security officer wanted his team to have the freedom to independently analyze threats. “We really needed a professional-strength solution that could help us locate and prove specific threats - where and when we wanted,” he commented, continuing, “We also wanted stronger reporting capabilities - both to assist with ongoing remediation and to support annual compliance audits.”

“Upon considering our options, it was clear that CORE Impact was the only choice,” stated the security officer. The product now enables his team to test for network vulnerabilities, identify what resources are exposed and determine if their security investments are effectively detecting and preventing attacks on customer data.

The Result
Direct Compliance with PCI Standard Requirement 11.3
By using CORE Impact Pro to perform network penetration testing on a regular basis, as well as after infrastructure and application updates, the organization is able to directly comply with Requirement 11.3 of the PCI Standard. “We run CORE Impact whenever we publish a new version of our website, which is about every four to six weeks,” stated the security officer, adding “And now that we’ve automated our penetration testing, we’re able to assess our security posture across over 2,500 servers - without over-extending our IT staff.”
Customer Success Story

Added Security for Other PCI Compliance Efforts

By performing automated penetration testing with CORE Impact, the company can independently test - and prove the existence of - network weaknesses. In doing so, they also bolster compliance efforts across a number of other PCI Requirements, including:

- **Requirement 6.1:** Ensure that all system components and software have the latest vendor-supplied security patches ...
  
  The IT team uses Impact Pro to test the effectiveness of every patch they install using the same attacks the patches are designed to stop.

- **Requirement 6.2:** Establish a process to identify newly discovered security vulnerabilities ... Update standards to address new vulnerability issues.
  
  While the company regularly performs vulnerability scans to identify potential network weaknesses, penetration testing enables them to take this a step further. With CORE Impact, the security officer’s team effectively distinguishes real vulnerabilities from false positives, allowing them to focus their remediation efforts on actual threats.

- **Requirement 11.1:** Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts ...
  
  Using CORE Impact, the organization is able to independently determine if attackers can actually exploit network vulnerabilities - with full control over the assessment process. “If we wanted to, we could test our network nightly. We can even target specific applications and servers on an ad-hoc basis,” the security officer stated.

- **Requirement 11.4:** Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.
  
  CORE Impact Pro enables the company to continually test the effectiveness of their IDS, IPS and other defensive technologies, alerting them to systems that may require new attack signatures and other updates.

Increased Preparation for PCI Audits

CORE Impact backs every penetration test with documentation of targeted networks and hosts, audits of all exploits performed, and details about proven vulnerabilities. The reports serve both to assist with remediation efforts and to provide proof of testing to PCI auditors. “We now have a foundation in place for documenting our vulnerability assessment and remediation initiatives throughout the year, making the annual auditing process easy and smooth,” the security officer said.

Decreased Network - and Company - Downtime

Prior to using CORE Impact Pro penetration testing at the organization often required the security officer’s team to take servers out of production and arrange for network downtime. “We know we can trust the product’s exploits and with CORE Impact the whole testing process is very discreet and stable,” said the security officer. With CORE Impact, the organization gets Commercial-Grade Exploits, which undergo a rigorous, in-house development and testing process and are guaranteed to be safe. He added, “On the flip side, by avoiding data breaches, we’re not only preventing downtime for our network, but also for my team - and the entire company as whole.”

Compliance with Both the Letter and the Spirit of the PCI Standard

The IT team knows that basic compliance with industry standards alone doesn’t necessarily guarantee network security. “While it’s nice to know that we’re compliant with regulations, it’s much more important for us to deliver on our promise to ensure information security for our customers,” the security officer stated, continuing, “Fortunately, CORE Impact helps us to both comply with the PCI Standard and honor our commitment to keep customer data safe.”