LINK
BYNET

CYBER
SECURITY

B-NETWORK OPTS FOR LINKBYNET FOR PCI DSS-COMPLIANT HOSTING

03

months only to roll out this project

90

of the standard's requirements accommodated by LBN

02

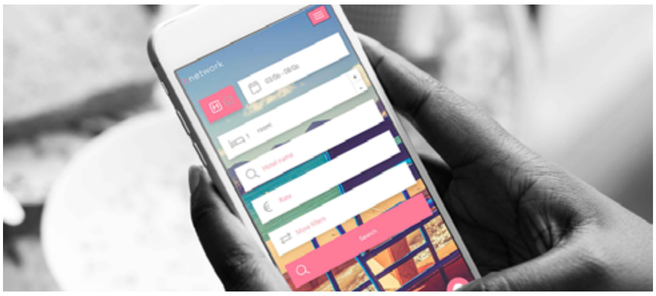
security software solutions installed via the AWS marketplace

"The switch to PCI-DSS and the migration of our infrastructure to the AMAZON WEB SERVICES cloud represented a major challenge for our internal organization."

Bruce Gonzalez,
IT Key Account Manager

bnetwork

Business case
Event logistic



B-network, leader in event logistics, entrusted Linkbynet with the facilities management of applications under the PCI DSS (Payment Card Industry - Data Security Standard).

In December 2015, one of B-Network's customers, specialized in hotel reservations, stated the need to gather and process information concerning its customers' credit cards in complete security while complying with the requirements of the PCI DSS (Payment Card Industry Data Security Standard).

Established by payment card suppliers, this security standard was introduced to tighten e-consumers' se-curity. To respond to this need, B-network adopted a solution developed and hosted in a data center. Se-veral months after deploying this solution, the cen-ter was destroyed by a flood. With the servers out of action, a fast response was needed!
B-Network promptly turned to a Cloud solution that would offer a better guarantee of continuous opera-tional maintenance.

B-Network decided on the Amazon Web Services so-lution, which it considered ideal for its needs. Indeed, AWS infrastructure and management tools are level 1 PCI DSS-certified (i.e. the maximum level) and cater to a considerable number of compliance issues. The AWS marketplace also serves to deploy security sof-tware more efficiently, more quickly, and in line with PCI-DSS requirements.

TRANSLATING THE REQUIREMENTS OF THE PCI-DSS

Linkbynet, a source of proposals for specific re-quirements concerning the PCI-DSS standard, ad-vised its client on the definition of its architecture and the security equipment to deploy in order to ensure compliance with the standard. Linkbynet oversaw the implementation of the ne-cessary security software tools, including a Web Application Firewall (WAF), intrusion detection and prevention systems (IDS/IPS), and a strong authentication solution. Meanwhile, an SIEM (Se-curity Information and Event Management) system was deployed to centralize and correlate the sys-tems and applications logs, and the reporting of alerts.

“To say that Linkbynet was an excellent partner is not enough; they were helpful and enthusiastic, gave key recommendations, and deployed the overall solution on time and in line with the requirements of our QSA. ”

Bruce Gonzalez,
IT Key Account Manager.

www.linkbynet.com

☎ +33 (0)1 48 13 00 00

✉ Info-linkbynet@linkbynet.com

In search of a facilities manager, specialized in AWS and cybersecurity

B-Network thus launched a request for proposals to find a facilities manager able to manage and structure an AWS environment while ensuring PCI DSS com-pliance.
Its choice went to Linkbynet for its expertise in cy-bersecurity, its certified AWS Advanced Partner status, and its proficiency in AWS Cloud managed services.

High-level configuration of security elements: the key to success

Counseling and implementing suitable security tools, configured on EC2, Cloud front and Route 53 solutions, represent the first steps towards ensuring an environ-ment’s security. However, these tools only offer any genuine added value if they are configured with the requisite granularity in order to guard against attacks, targeted or otherwise. This is where the Linkbynet experts step in to effectively configure these software components, which will subsequently serve to raise alerts or counter attacks in the operating phase.

Once the security equipment has been properly confi-gured, Linkbynet’s added value is to ensure that the level of security reached is effectively sustained. For this purpose, vulnerability scans are regularly carried out. These scans serve to detect security flaws and to mitigate them by deploying the appropriate corrective measures, or tightening the configurations.

Conclusion

The environment advocated by Linkbynet and AWS, and the high-level configuration of the secu-rity tools underwent a PCI-DSS certification audit by an external auditor: this audit was successful-ly passed. The watch carried out by Linkbynet’s security experts ensures that B-network always meets the security requirements and business issues of its customers with the utmost precision.