blakemore retail

NNT Compliance Case Study: AF Blakemore

AF BLAKEMORE SAVES AN ESTIMATED £200K IN ASV SCANNING COSTS

THE CLIENT

AF Blakemore distribute goods to nearly 1,000 SPAR stores in the UK, as well as running one of the UK's most successful and largest SPAR franchise operations

In common with other retailers around the world, PCI DSS has been a significant headache during the last decade since its introduction in 2004.

THE CHALLENGE

Retail is a business sector that always works on tight margins and cost control for any IT investment is subject to close scrutiny with value for money and return on investment carefully assessed.

There are seldom any shortcuts when it comes to security, especially when under PCI DSS Validation Requirements, Tier 1 Merchants (those transacting more than 6 million transactions each year) must be independently audited for compliance with the standard by an authorized Qualified Security Assessor (QSA).

THE SOLUTION

AF Blakemore needed to balance the need to fully observe all sections of the PCI DSS mandate, while maintaining the highest levels of security and integrity of IT Systems, whilst at the same time minimizing expenditure and resource requirements - this is where NNT have been able to help.

"When we looked at ASV scanning cost projections for our estate the numbers were potentially huge" says Jim Curtis, PCI DSS Consultant for AFB. ***"The other requirements for PCI DSS such as reviewing and backing up event logs, file integrity monitoring and device hardening were already looking to be expensive too, but the NNT solution solved everything for us."***

"NNT Change Tracker was recently awarded a maximum 5 out of 5 in Secure Computing's Group Test and combined with NNT Log Tracker, provides PCI DSS Merchant's with the most cost-effective and easy to use Compliance Management solution available", Russell Willcox, Chairman NNT.

Using built-in PCI DSS device hardening templates and continuous configuration state tracking ensures that EPoS and Back Office servers remain 'hardened' at all times.

Crucially, this means that in terms of their PCI DSS vulnerability scanning obligations, AFB need only scan a small percentage of store sites, saving money and time without any compromise to security.

Jim Curtis concludes, "***We estimate savings of 200K a year by taking this approach.***"

KEY FACTS - AF BLAKEMORE

- AF Blakemore currently supplies more than 700 stores across England and Wales
- Following the acquisition of Tates Ltd in 1994, AF Blakemore's "own-stores" division encompassed more than 200 SPAR shops, a figure that has now grown to 280 stores
- AF Blakemore merged with Capper & Co. to create a combined business of 7,990 personnel serving a total of 1,096 stores made up from franchised and own stores
- Around 5,500 people are employed by the company, with a turnover in excess of £800 million per year
- As a tier 1 merchant, AF Blakemore is subject to the PCI DSS 3.2 and must be audited for compliance every year by a registered PCI DSS QSA
- PCI DSS V3.2 11.2.2 and 11.3 mandates that quarterly external vulnerability scans and annual external and internal penetration testing must be performed
- However, big savings can be made where the estate can be shown to be maintained in a provably hardened state, meaning that just a small, statistical sample of stores needs to be scanned to prove all stores remain hardened (PCI DSS 3.2 Report Section 2)
- In summary, NNT was able to save an estimated £200K per annum by reducing the vulnerability scanning requirements scope

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative. W: www.newnettechnologies.com E: info@nntws.com

Visit www.newnettechnologies.com for more information and trial software