NNT Compliance Case Study: Wonga

LEADING FINANCE PROVIDER WONGA MEETS PCI COMPLIANCE NEEDED USING NNT

THE CLIENT & CLIENT CHALLENGE

London based digital finance company, Wonga, has rapidly become one of the worlds most innovative and successful credit providers. Serious about their commitment to responsible lending and putting the customer at the heart of everything they do, the company has grown at an impressive rate since its inception in 2007. Wonga's strapline of 'straight talking money' for short term cash loans encapsulates its approach to providing credit with simple, transparent and flexible services.

Automation is a key word for Wonga. By using fully automated and real-time risk technology to process thousands of pieces of data, objective lending decisions can be made instantly. This automated and real-time risk approach goes further than loan decisions. By applying the same ethos to securing its IT infrastructure Wonga has ensured that the thousands of pieces of sensitive financial and personal information stored within its IT environment is protected from both internal and external IT security threats.

As a consumer credit organization dealing with financial transactions Wonga must adhere to the PCI DSS, a complex set of regulatory requirements, often viewed by companies as an adjunct to the existing IT security strategy. For Wonga, who are a tier 1 merchant processing more than 6 million transaction a year, validation of compliance is completed annually by a QSA (Qualified Security Assessor) via an audit.

Generally positive, the audit did however highlight a lack of hardening standards for servers and network devices, as well as the inability to automate the process of gathering and correlating event logs, reporting relevant changes to system and application files, configuration settings and other key system attributes in an audit ready format. Given the breadth and complexity of PCI DSS requirements it is common for Merchants subject to the DSS to need help in understanding and implementing measures necessary to safeguard their customers' card data and in turn, protect their company brand value.

THE SOLUTION

It was at this point that Ayo Obasanya, Infrastructure Manager at Wonga began looking at the different approaches, technologies and suppliers that could help secure the environment and achieve PCI Compliance.

Ayo explains the search, "***We considered a number of options. We already had a log management solution in place to gather event logs and show file changes but it became apparent that this type of solution just didn't give us enough detail, we needed something that would correlate the information and flag up changes that could prove to be hazardous. We also looked at firewall policy management but the solutions offered nothing for servers, and all of the other leading Change and Configuration Management vendors were generally complex and expensive.***"

Ayo concludes, ***"We knew we needed one solution that could cover all the bases and that's when we came across NNT. Their solution gives us everything we need, it even identifies what has changed within the files and registries, who made that change and if it was planned or unplanned. This saves us a huge amount of time and effort in understanding what is going on in the environment, there's no need to shift through endless infor-mation and it ensures we don't miss anything critical in the mass of data.***"

Wonga quickly identified the wider value of NNT's integrated SIEM, CCM and FIM solution in protecting the environment from both external and insider man threats. Realizing that NNT would bring PCI DSS under the umbrella of the existing IT security strategy, rather than operate as a standalone compliance process, NNT's Change Tracker Gen7 R2 and Log Tracker has been deployed beyond the in-scope PCI infrastructure to cover the entire IT estate of 750 devices, a heterogeneous environment that includes Windows and UNIX servers, Cisco and Dell network devices and checkpoint firewalls.

NNT provides Wonga with prebuilt hardening standards for their network devices, Windows and UNIX platforms, meaning they get full device coverage in one easy to use system. This is combined with, change management and change detection that ensures 'once secured and hardened' all devices remain that way. Intelligent log analysis and auditor ready reports are also used to sure up and demonstrate PCI DSS compliance.

Wonga now has a secure, stable and PCI compliant IT infrastructure that can detect unplanned changes in real-time, alerting to any unusual activity that can be dealt with appropriately before any damage can be done.