
Neustar Research Reveals Data Volumes and Network Stress to Be Top IoT Concerns

Dec 8, 2015

Fresh research commissioned by Neustar, Inc. (NYSE: NSR), a trusted neutral provider of real-time information services, into the many guises of the Internet of Things (IoT) has revealed that although being the topic du jour of 2015, IT departments' No. 1 concern is that the resulting explosion in data volumes will start to overwhelm their networks in 2016, leading to security concerns around keeping all the extra data safe. The report, compiled by independent analysis firm Quocirca, found that the scaling out to many thousands of devices per organization clearly represents a wealth of new opportunities but highlighted the importance that the same security rigor and vigilance applied to *traditional* IT devices needs to be extended to all *connected* things.

The full report from Quocirca can be read here:

https://hello.neustar.biz/2015_quocirca_uk_iot_report_security_lp.html?utm_medium=press%20release&utm_source=neustar&utm_campaign=201512-security-services-quocircaiotreport-pressrelease&ucid=7013900000mnraaau

The IoT is an evolutionary concept with as much power to improve existing or brown-field business processes as it does to create new green-field ones. Many equate the IoT purely to machine-to-machine (M2M) communications, but it is also about how humans interact with machines either through human-to-machine (H2M) such as industrial equipment or consumer devices, or machine-to-human (M2H) for things like digital signage. One thing is for certain, all this activity adds up to a huge number of devices with the overall average per individual UK organization expected to run into the thousands over the next 12 months. All these devices will be attached to a variety of networks resulting in increased stress on both existing and new networks.

“The new UK-focused research contained in this report highlights that businesses looking to deploy IoT should consider a decentralized security and management model, as this would have the combined effect of reducing data volumes and relieving the considerable strain on networks,” said Hank Skorney, SVP Internet of Things for Neustar.

The many guises of IoT

Although the report – compiled from the responses of 100 senior UK IT managers – shows that security is considered highly important by all respondents, it is clear that no business can ignore the wide range of issues arising from the growing numbers of network attached devices that constitute the IoT. Below is a breakdown of key findings and statistics from the report:

- *Relevance*: a small number (3%) think the IoT is overhyped, but the overwhelming majority say the IoT is already impacting their organization (37%) or will soon (45%).
- *Personal to Global*: respondents believe the IoT is expected to scale up through vehicles, buildings, cities to the national and global level. Management and security capabilities put in place to support IoT must operate at these scales.
- *Design*: effective management and security is only possible through good design. 66% of respondents see viewing IoT deployment being a series of hubs that interoperate with spokes on closed networks, making network configuration and security more manageable.
- *Security*: Security starts with identity. 47% of respondents are already scanning IoT devices for vulnerabilities, another 29% are planning to do so. When asked about the capabilities they feel are most important for authenticating the identity of devices, nearly all see DNS services as playing an important role. More experienced users supplement these third party registry and IoT database services.

“Sceptic or otherwise, the IoT is now relevant to all organisations. Whether IoT applications are deployed to help IT function, driven by lines of business or through devices introduced by end users, various practices will need adapting to accommodate the millions of things involved which will, over time, dwarf the number of traditional IT endpoints,” explained Bob Tarzey, Analyst & Director, Quocirca. “These challenges can be minimized through thoughtful design and the use of hubs, in addition to new networks, management tools and security capabilities to get the most out of the IoT. Quocirca’s research suggests that the cost of supporting investments can be justified by the business value derived from newly IoT-enabled applications.”

Security strategy – decentralized management

Many IoT security issues such as data protection, botnet recruitment and DDoS-style attacks on IoT enabled processes are addressable through adapting and scaling measures that are already in place for existing IT infrastructure. For instance, 39% of respondents were found to have DDoS protection in place, with another 31% planning a deployment. However, the report found that there is not much difference between major IoT users and sceptics as DDoS attacks have been an issue for many years. More could be done to address the problem.

The adoption of a decentralized security and management model where a gateway needing a unique IP address controls communications with the outside world (for example, network routers, set top boxes, smartphones etc) which in turn communicates onwards with remote devices which do not need unique IP addresses, avoids the need for each device to have a unique IP address. This approach can work at scale, making the selective,

effective and cost efficient deployment of IoT security more straightforward as scanning can be carried out using the same processes in place for existing IT endpoints. 35% of experienced IoT users already recognize the value of such an approach.

Rodney Joffe, Senior VP and Fellow at Neustar, said: “As more and more devices become tied into the Internet every day, the security threat will continue to expand to new industries and areas and so there needs to be a focus on security practices before any other. However, this proliferation of IoT connected devices will put pressure on manufacturers of these devices to get to grips with IoT security control.”

The full report from Quocirca can be read here:

https://hello.neustar.biz/2015_quocirca_uk_iot_report_security_lp.html?utm_medium=press%20release&utm_source=neustar&utm_campaign=201512-security-services-quocircaiotreport-pressrelease&ucid=7013900000mnraaau

About Neustar

Neustar, Inc. is a trusted, neutral provider of real-time information and analysis to the Internet, telecommunications, information services, financial services, retail, media and advertising sectors. Neustar applies its advanced, secure technologies in location, identification, and evaluation to help its customers promote and protect their businesses. More information is available at www.neustar.biz