Dhwani Parekh
Marketing Analyst
ManageEngine

IoT: Waking up from the Network Admin's nightmare

Dhwani Parekh, Marketing Analyst, ManageEngine examines the major challenges that will be thrown up in terms of managing IoT devices for organisations

If statistics from Gartner and others are anything to go by, the Internet of Things is the certain future. In a Gartner study from March 2016, almost a third (29 percent) of the surveyed organizations are currently using IoT. And an additional 14 percent planned on implementing the technology by the end of 2016.

As organizations move towards IoT adoption, they will also need to brace themselves for its adverse consequences. One of the parties facing these consequences will be the network administrator. Here are three major challenges a network admin will face with the proliferation of IoT:

1. Network security

If you ask a network admin who handles IP devices on the network how well the security is holding up, you're bound to hear a sarcastic comment and an exaggerated sigh. With new hardware, software, and patches constantly being injected into their precious network, they are already stretched thin. Imagine their horror if the organization decided to connect all the things, or sensors and devices, to the network. I think we can all agree they would deserve a pay raise and fast.

Securing the IP devices on the network is already quite a task. With IoT in the picture, the number of devices will shoot up in a short amount of time. Securing the gateways, or the IP enabled devices that connect the sensors and devices to the network, becomes critical. But even that might not be enough. In his book RIoT Control, Tyson Macaulay, a security veteran, predicts that local devices, other than being connected to the cloud, will also have the ability to communicate with each other through the gateway. That's when securing the gateways to protect the data in the cloud will fall short, because an infected device could communicate with local devices and render them useless, or worse—hacked.

A recent article on Wired opens our eyes to the extent of such a network security threat that early IoT adopters are facing. It points out an unnoticed but deadly consequence of a security breach in an IoT environment. To quote the article, "One major concern is that, unlike having your Facebook account hacked, the average person will likely never realize that their IoT devices have been compromised." Security being one of the major problems faced by network admins, it would be safe to assume that a sound security system would have already been put into use before adopting

IoT. A continuous monitoring system, though, would be the best option to overcome this particular hurdle.

> ***"With updates and releases by different vendors for different devices already being managed by the network admin, adding IoT devices to the list will definitely prove taxing. Not only will the network admin be facing these challenges, so will the regulatory bodies themselves."***

2. Auditing and compliance

Regulations such as HIPAA, PCI DSS, SOX, FISMA, GLBA and more demand up-to-date information security. The advent of IoT is bound to bring about reforms and amendments in these regulations, forcing organizations to keep up.

Gartner predicts a 225 percent rise in the number of IoT devices over the next four years. If you think your setup would (most likely) account for one of those numbers contributing to this statistic, then you have already begun the preparation. Any organization with a fairly large number of IT assets will already be facing complexities when trying to comply with regulatory requirements. As these organizations adopt IoT, the complexities increase thanks to different regulatory requirements being introduced for the technology. Maintaining compliance with these regulations, especially as they are renewed and updated on a regular basis, will be challenging.

With updates and releases by different vendors for different devices already being managed by the network admin, adding IoT devices to the list will definitely prove taxing. Not only will the network admin be facing these challenges, so will the regulatory bodies themselves.

As these regulatory bodies come up with better reforms and regulations, network admins strive to fulfill the requirements of compliance auditors by producing the corresponding compliance reports that demonstrate the security measures that protect their network from being compromised.

3. Bandwidth management

With the huge number of applications and services running on a network in an organization due to virtualization and cloud computing, networks are now overburdened. This has brought the bandwidth management issues faced by the majority of the IT departments across industries and organizations to the forefront. The networks, already battling with these new technologies, are forced to flex even more to incorporate the BYOD technology. With employees connecting their mobile phones, laptops, tablets, smart watches, and smart fitness bands, the network had to be ramped up with efficient protocols, local caching, higher speeds, more network cards, and so on. Adding the pressure of IoT into this mixture is a sure fire way to tip the delicately balancing network of the organization.

If we were to take into account the smaller IoT devices such as the weather reporter or the monitoring devices that send mere megabytes of information every few hours, then bandwidth utilization would not be such a problem. But if we are to take into consideration high data usage over the networks such as remotely controlling a truck used to transport ore in mines, something this Swedish pilot program has ventured into, the whole scenario takes a turn for the worse. Next will be smart billboards fetching 4k resolution videos for advertisements. Imagine handling that kind of traffic on your current network.

IoT as a technology is still in its nascent stage, or as a one article puts it, "Right now the Internet of Things is an awkward teenager." As it grows, which we are promised will be fast, newer challenges will follow. And as mentioned above, the enterprise network is still coping with the recent adoptions of AI, virtualization, and hybrid computing.

With all the issues and challenges already being discussed across the globe, you might have started working towards strengthening your network. As you prepare your organization for IoT, you might want to add these to your checklist!

- Thwart security challenges by proactively monitoring the devices across the network. Choose a monitoring tool that has the capability to drill down to the deepest details, making both active and passive monitoring possible simultaneously strengthening the security of the network.

- Auditing and compliance for IoT needs to be handled dynamically. Opt for vendors that upgrade and scale corresponding to the changes in the environment. Choose tools that automate report generation and simplifies alerts to avoid audit complexities.

- As you get ready for higher bandwidth usage with IoT in the picture, it would be wise to automate prioritization of the same within the network. This helps optimize bandwidth usage to avoid bottlenecks during peak times.

- Integrate all your monitoring tools to get central control over the entire network to ease the inclusion of IoT devices through a single tool. Monitoring these devices along with the rest of the devices on the network would help map every device and determine the root cause of any unanticipated incidents.

When your IT and your organization is properly prepared, you can turn what could have been an IoT nightmare into a sweet dream of success with connected devices, automation, and competitive advantage.