Four Strategies to Improve Network Security and Unlock IoT Innovation

By: Ray Watson

As the scale of the Internet of Things (IoT) market continues to grow exponentially, enterprise technology spending in the space shows no sign of slowing down.

According to a recent McKinsey report, by 2020 the IoT market will be worth $581 billion for information and communications technology-based spending alone, growing at a compound annual growth rate between seven and 15 percent. In addition, the discrete manufacturing, transportation and logistics, and utility industries are projected to spend $40 billion each on IoT platforms, systems and services by 2020.

This flood of spending in IoT will enable never-before-seen business speed and functionality. As enterprise decision-makers are dropping big bucks in this market, however, they should keep in mind that there will be a series of bottlenecks that will obstruct the flow of IoT innovation across the marketplace. The largest of these bottlenecks are likely to be security and deep network visibility.

The value of an optimally connected IoT environment is well-known. Networks of sensors can be applied to manufacturing equipment, for example, to transmit data about their condition so that they can be serviced before a breakdown. But as you begin to apply these sensors to larger and broader networks, providing deep visibility and applying advanced analytics becomes increasingly important. Additionally, distributing networks across a wide area with lots of devices spreads network monitoring resources thin and forces IT teams to make tough decisions about where and how to prioritize security efforts. This diffusion leaves networks more vulnerable to cyberattacks and threatens the ability of the system as a whole to function as it is intended.

Considering the significant IoT challenges to come, the best way to maximize ROI when investing in IoT is to recognize which capabilities and resources are most essential for network functionality and prioritize acquisitions accordingly. Here are four strategies for effectively prioritizing the most critical aspects of the network to improve enterprise's IoT strategy.

Look to software-defined networking to "agilize" your enterprise

Software-defined networking (SDN)—which centralizes control of the network through intelligent software—is an excellent starting point for enterprises to improve network agility and visibility.

With SDN, enterprises can allocate dedicated resources to IoT infrastructures without impeding other business processes. SDN's advanced segmentation gives users the ability to seamlessly create virtualized environments where IoT network traffic is separated from critical network infrastructure for security and management purposes. Additionally, centralized control of the broader network enables controllers to provision resources for peak-load demands as needed and lets them streamline their management processes. These types of user-friendly operating consoles are the secret to deploying and managing IoT technologies while simultaneously minimizing their security vulnerabilities.

Dive deep into your network by enhancing visibility with analytics

In order to effectively manage an expansive ecosystem of connected devices, IoT-created data needs to be stored, processed, analyzed and acted upon in an efficient manner. IoT devices generate and transmit huge quantities of data, the vast majority of which is never used or analyzed in an effective way to improve the system as a whole. An enlightened approach to IoT management involves finding ways to view all of the data and effectively processing it by leveraging advanced analytics. This analytical approach can help identify pain points within the network and recommend ways to create a more efficient system overall. This approach focuses resources on data that could have security implications and overlooks superfluous information that presents less of a threat.

Fortunately, analytics and machine learning thrive in environments that possess extreme volumes of data. Leveraging advanced analytics in IoT-scale environments can help point out where things are working, where systems can be improved, and where cyber vulnerabilities may exist. Doing so can also provide evidence-based recommendations on how to best improve the overall network.

Continuously monitor and secure your infrastructures

When establishing IoT devices and systems at the enterprise level, IT pros need to be well-attuned to the security threats that could be unleashed by extending a network. In order to mitigate these risks, enterprises should proactively take steps to prevent compromises in their systems by creating policies for connected devices, security monitoring, protection against botnets and security patches for all connected devices. By coordinating segmentation strategies and security policies, it is possible to dynamically monitor network behavior in response to typical IoT events and report anomalies that could indicate a security threat.

These comprehensive security ecosystems based on machine learning and behavioral analytics are able to detect early indicators of network infiltration. Additionally, 24/7 security monitoring by a team of experts can accelerate the processes needed to identify attackers, watch for lateral moves, and mitigate threats before they cause extensive damage.

Accommodate bandwidth needs through SD-WAN

Ensuring a network can adequately support the advanced needs of IoT is critical, particularly as global markets become increasingly competitive. An increase in data driven by more connected devices will require more bandwidth on the network to enable the sharing, transport and storage of that data. Therefore, in the new IoT management arena, enterprises will demand a way to monitor and control the amount of bandwidth their system needs, and flex accordingly. A robust managed SD-WAN service is well-suited to serve these needs.

The implications of establishing a robust and secure network serve more than just the system's functions. Fifty-three percent of enterprises expect IoT data to assist in increasing revenues in the next year. The data is showing increasingly clear signs that the necessity to and ultimate advantages of investing in a managed software-defined network are clear.

Practices in action: How Teknion became an IoT disruptor

Using global cloud and IoT strategies, the high-end workplace furniture manufacturer Teknion shifted to a new analytics-based business model. With a secure software-defined platform, the company established industrial IoT capabilities to collect massive amounts of data from its equipment and applied advanced analytics to enhance its understanding of the larger system. The project resulted in dashboards that help leadership make real-time decisions about usage and repair scheduling. Along with the network's ability to create an unlimited number of virtual environments where R&D teams can safely test and improve the latest technologies, these insights are part of Teknion's innovation incubator.

This optimized IoT environment resulted in a more agile IT infrastructure that helped accelerate cloud migration and empowered a sophisticated overall strategy. It also simplified Teknion's IT complexity with a global software-defined network platform that enhanced network efficiency with on-demand bandwidth and deep analytics. Most importantly, the use of a software-defined network reduced the equipment Teknion needed to manage its expansive network, thereby also reducing maintenance and support costs.

What's ahead for IoT

IoT is still on the rise, but its effect across consumer and commercial fronts has already made a significant impact. Through the numerous and diverse uses for IoT, tomorrow's savvy enterprises will benefit from monitoring and analytics capabilities never before possible. Perhaps some of the most exciting areas of potential in this technological growth area are the practicalities of application and implementation that can assist enterprises in functioning at a higher capacity.

And yet, IoT is not simply a plug-and-play endeavor. It will still require augmentation from robust and time-tested network management technologies like software-defined networking and SD-WAN to make it all happen effectively.

With these technology forces working together, IoT will usher in a new era for enterprise technology that will change the way we store, manage and protect data, as well as challenge us to rethink the way we view the cloud, network security, and big data.