The regional consumer IoT market is expected to grow at 35 percent CAGR between 2015 and 2020, reaching $7.53 billion in 2020.[23] This growth is driven by factors such as rapid urbanization, the growth of the middle class, and technology and device proliferation.

In ASEAN, several member states have also launched programs to increase their use of IoT, particularly in urban environments. Malaysia's MIMOS, the national ICT R&D center under the Ministry of Science, Technology, and Innovation, released its National IoT Strategic Roadmap in 2015. Singapore's Smart Nation, launched in 2014, includes a range of ongoing initiatives that utilize a countrywide IoT platform to improve citizens' quality of life and accelerate innovation. Bangkok, Jakarta, and Ho Chi Minh have also launched smart city programs.

> "In the last few years, the transportation sector has seen the proliferation of IoT and connected cars, which have the potential to be ubiquitously connected and form a far larger attack surface for DDoS—multiple times larger than what we have seen in the Mirai worm example."
>
> **—land transport authority in an ASEAN country**

IoT endpoints tend to be unsophisticated devices, representing low-hanging fruit for attackers who will identify the weakest link in a connected network. The network, or the edge that connects the endpoints to the platforms, is also vulnerable. IoT attacks are already extremely prevalent in Asia. According to NTT Security's *2017 Global Threat Intelligence Report*, 60 percent of all IoT-based attacks in 2016 originated from Asia, most likely because of the historically vulnerable profile of products in Asian markets

In this context, a secure access policy and software-defined segmentation is vital The network can be a security sensor, giving visibility of network traffic from these proliferating devices and ensuring access is granted and usage enforced using software defined segmentation To implement effective and efficient application segmentation, it is critical to understand how application components are communicating with each other, what infrastructure services they are dependent on, and how the component clusters are grouped together Rich telemetry and unsupervised machine learning can be used to achieve this This application insight and dependency form the basis of the segmentation policy, helping to contain a breach by ensuring that attacks do not move laterally.