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.

The accelerated adoption of multi-cloud computing

Enterprise IT operations are also shifting to a new operating paradigm with multi-cloud computing, where each unique cloud environment introduces new vulnerabilities. Not only are there multiple access and authentication nodes to manage securely, cloud platforms themselves represent attractive, well-connected targets for malicious hackers. Since the end of 2016, more hackers have been targeting cloud systems, with attacks ranging in sophistication, as they work relentlessly to breach corporate cloud environments.[24] Security professionals also identify cloud infrastructure and mobile devices to be among the most challenging to defend against attacks.

Segregating and protecting memory spaces prevents applications in cloud environments from accidentally interfering with one another's data or malicious software from being able to see and modify it at will. Recent news releases have highlighted two related vulnerabilities—Meltdown and Spectre—that allow a malicious application running on a computer to peek into the memory of another application on the same computer and interfere with it. Meltdown makes the segregation and protection process unreliable, while Spectre essentially tricks applications into accidentally disclosing information that would normally be inaccessible, safe inside their protected memory area. These vulnerabilities are most devastating in public cloud environments where applications from different customers often end up running on the same physical computer. End-to-end encryption, a security technique where data is encrypted before it even gets to the cloud and is then decrypted by clients when it is received from the cloud, offers a solution to the challenge. As a result, it no longer matters whether data is accessed by attackers in the cloud—because even if it is, it is not useful. It is encrypted and cannot be decrypted by the attacker without the keys, which are not present in the cloud that was attacked.

The growing share of encrypted traffic

An additional complexity is the increasing opaqueness of the data flow itself as the use of encryption grows. A growing share of enterprise network traffic is now being encrypted, creating gaps in security effectiveness that companies cannot afford to ignore. Gartner predicts that by 2019, 80 percent of Internet traffic will be encrypted. Encryption technology has enabled much greater privacy and security for enterprises that use the Internet to communicate and transact business online. Mobile, cloud, and Web applications rely on well-implemented encryption mechanisms, using keys and certificates to ensure security and trust. However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to

[24] *Cisco 2017 Annual Cybersecurity Report*