INTRODUCTION TO ENDPOINTS: BENEFITS AND USE CASES

Connected devices, aka the Internet of Things (IoT), are all around us. Enterprises are connecting and automating things, which were previously dumb terminals, into intelligent devices that can talk and act with other systems. In this article, we will focus on hardware endpoints, which are also known as IoT devices.

What's an endpoint?

Endpoint refers to a unit at the end of a communication channel. It can be a device, tool, service, application, or node accessed over a connected network. Traditionally, endpoints of a communication network have been the modems, routers, switches and host computers connecting to the TCP/IP network. Endpoints have emerged as a key enabler of automation technologies and extending computing capabilities from centralized backend systems to the edge of the network.

Specifically, IoT endpoints have the following characteristics that make them an important part of the modern enterprise IT strategy:

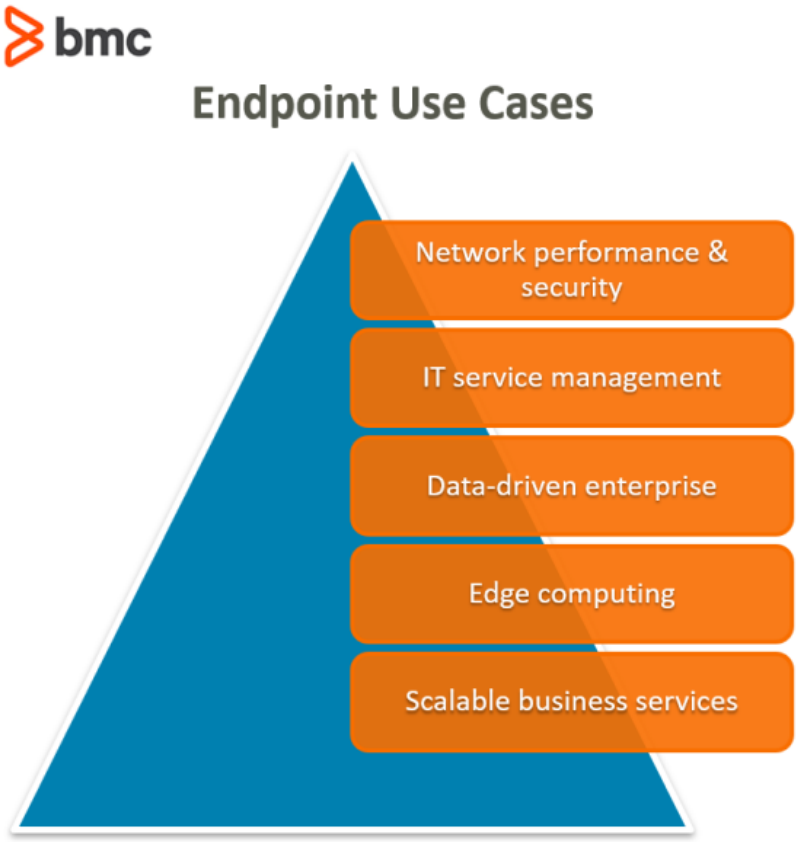
- **The extended network.** Endpoints are essentially an extension of the internet as we know it. Endpoints extend the purpose of the internet—but to things instead of humans. Connected things, or endpoints, can consume and act on the information they receive from the internet and talk to other endpoints or backend systems across the network.
- **Endpoints as sensors.** Endpoint devices operate as a source of data. The data can be specific measurements such as temperature or logs of the network traffic observed at nodes of the

endpoint. Collected and analyzed from several endpoints, this information contains valuable insights that can drive critical business decisions.

- **Endpoints as edge computers.** IoT endpoints extend the computing capacity of the network and limit the amount of data that must be communicated from a host device to the backend network for computation requirements.
- **Endpoint functionality.** Endpoint devices are designed to perform specific, limited functions. A typical IoT endpoint is a microcontroller-based processing device that can be programmed to perform a desired computation functionality.
- **IoT endpoints are installed at scale.** Thanks to their low power consumption, endpoints can perform computationally inexpensive tasks across the distributed network.
- **Automation.** One of the most popular applications of IoT endpoints is to enable automation capabilities. An endpoint can be connected to a mechanical system that receives instructions to perform an automated maneuver.
- **The security challenge.** Vulnerable endpoint devices are responsible for a majority of security infringements and data leaks. Endpoints tend to receive little attention when it comes to security. According to a recent survey among IT operations and security professionals at midsize and large enterprises, less than 50% said they can patch vulnerable devices against zero-day attacks proactively.

Business use case for endpoints: the benefits

IoT endpoints have changed how businesses interact with their audience and its surrounding environment. It presents new ways to monitor the physical world and generate massive streams of insightful data about their end-users. These interactions are further mediated by machines and things that gain intelligence with the ability to connect to a network, receive information, and act accordingly. As a result, a connected endpoint presents immense value across a range of business focused applications in the following domains:



- **Network Performance and Security.** IT and ICT infrastructure are the heart of virtually every business service. The availability and performance of a network defines how well a business service can reach its end-users. These parameters are monitored continuously by endpoint sensors deployed at the edge and nodes of the network. The generated data logs can help organizations identify network traffic for anomalous behavior and suspicious activities, capacity and resource allocation, and SLA performance.
- **ITSM.** Connectivity brings both opportunities and challenges in the ITSM space. The growing number of connected devices used to access a service can overwhelm the IT Service Desk to serve its customer base. At the same time, IoT empowers the Service Desk to automate and assist in ITSM tasks such as service provisioning, knowledge management, and other ITSM functions.
- **Data-Driven Enterprise.** The modern business is data-driven. Access to the right information gives businesses the edge against competition that relies merely on experience and intuition to develop their business strategies and decisions. IoT endpoints provide an insightful view of end-user activity in the field.
- **Edge Computing.** Computing at the edge of the network, close to the source of data, endpoints deployed at scale can generate a deluge of information. The transfer of this data to backend systems for storage, processing, and access adds to the capacity requirements of the network and IT infrastructure. By computing on the edge, businesses can serve their end-users based on real-time local information without the latency that comes from sending data to and from the backend servers.
- **Scalable Business Services.** Progressive organizations add value to their service with the ability to scale. When a new feature is launched and the service updated, endpoints can be reprogrammed to reach a wider user base at scale. As a result, business services accessible by connected endpoints can be tailored, updated and improved based on evolving end-user response.

State of endpoints in 2020

IoT endpoint integration has been widely adopted for decades. The Gartner Hype Cycle registers this technology trend at the Slope of Enlightenment maturity phase. Billions of devices are already connected to the Internet and serve critical tasks in our daily lives, including HVAC, home automation and mobile device controls. Naturally, business organizations are responsible for managing endpoint security, especially considering the vulnerability of IoT devices.

However, IoT devices continue to lead security concerns and businesses according to recent reports:

- IoT endpoints are the “top driver of internet attack traffic”. (F-Secure)
- IoT endpoint devices face an average of 5,200 attacks per month. (Symantec)
- Endpoint devices are commonly used in conducting Distributed Denial of Service (DDoS) attacks. In 2018, DDoS was the third most common threat. (Symantec)
- 61% of organizations have already experienced an IoT security incident. (CSO Online)
- More than half of IoT devices are vulnerable to medium to high severity attacks. (Palo Alto Networks)

Additional resources

For more information, read the following BMC blogs:

- Introduction to Enterprise Security
- How IoT is Impacting ITSM
- Introduction to BYON (Bring Your Own Network)