Data & Endpoint Security

FTVETI

ICT @ FTVETI

Objectives

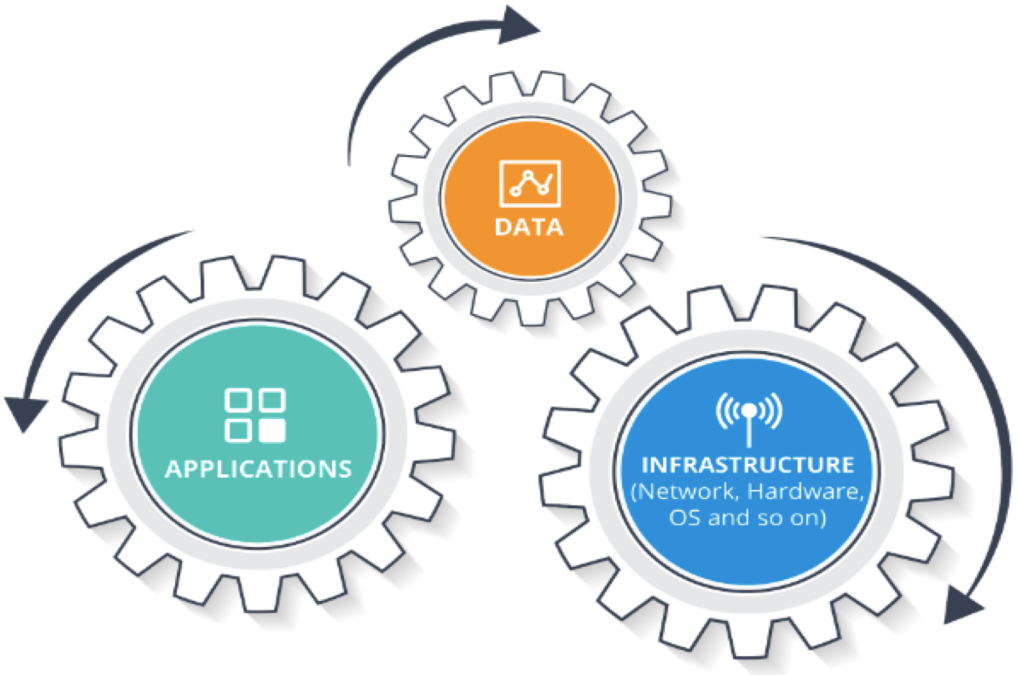
After completing this unit, you should be able to:

- Appreciate Data Classification principles
- Understand the need of Maintenance of an Asset inventory from information security perspective
- Understand the meaning of Computing Endpoints
- Delve into selected Endpoint Security risks & controls
- Understand the basics of SANS Endpoint Security Maturity Model
- Identify features of today's comprehensive endpoint security solutions

Enterprise Information

Enterprise Information – Constituents

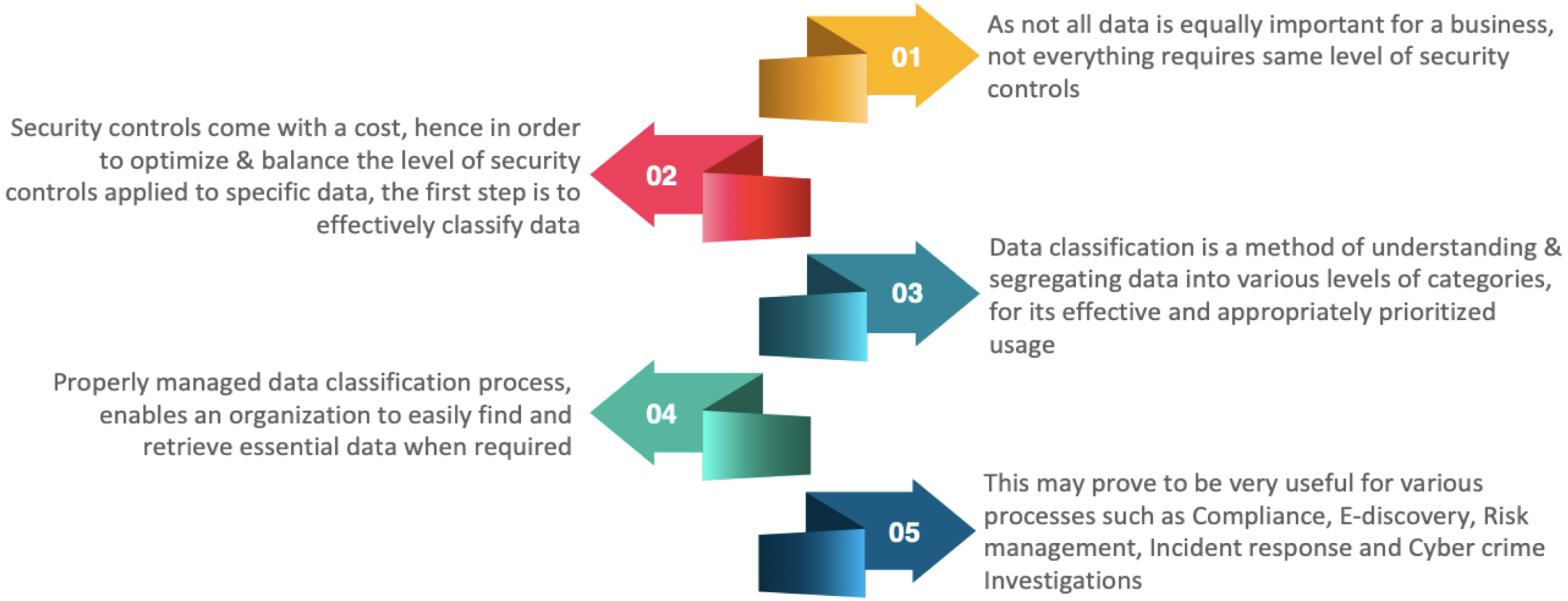
- Elements that constitute the enterprise information are: **Data**, **Applications** and **Infrastructure**



- Management units for the Enterprise Information are: **Portfolio**, **Program** and **Projects**
- Governance units for the Enterprise Information are: **Policy**, **Procedures**, **Guidelines** and **Standards & Processes**

Data Classification

Need Of Data Classification

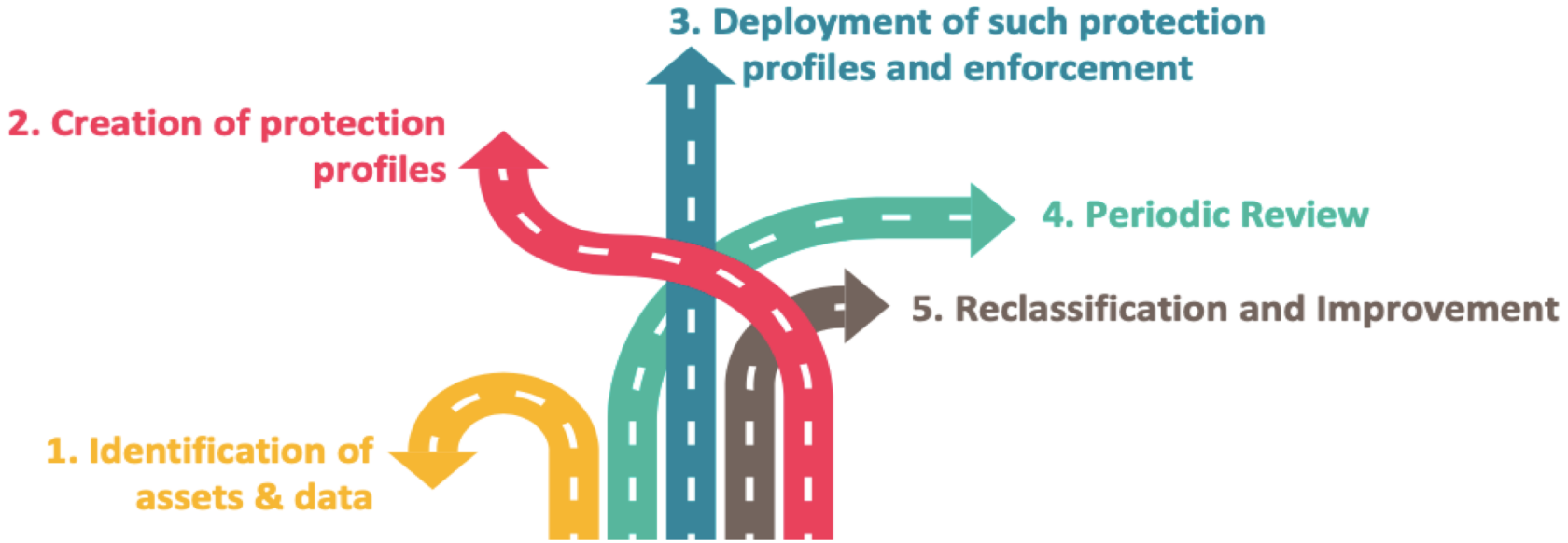


FTVETI

ICT @ FTVETI

What Is Data Classification?

- A **Data classification** scheme is not only meant to be used by IS/IT teams but is recommended to be used by all data, applications, infrastructure & process owners in the organization
- Data Classification theme should match closely with the business objectives, risk assessment, organization culture, processes, governance, org. maturity and so on
- A typical data classification exercise is based on the following steps:



Examples Of Data Classification

- **Example 1:** Military uses various levels of data classification such as:
  - Top Secret
  - Secret
  - Confidential
  - Restricted
  - Unclassified

- **Example 2:** A general template for Data Classification in an organization may include the following levels:
  - Secret
  - Confidential
  - Internal Use Only
  - Personal
  - Public

Asset Inventory

01 Active management of all hardware devices connecting on the organization's network is the key

02 This helps in ensuring that only authorized devices get access, but the unauthorized /rogue /non-compliant devices are found early and prevented from gaining access into the network

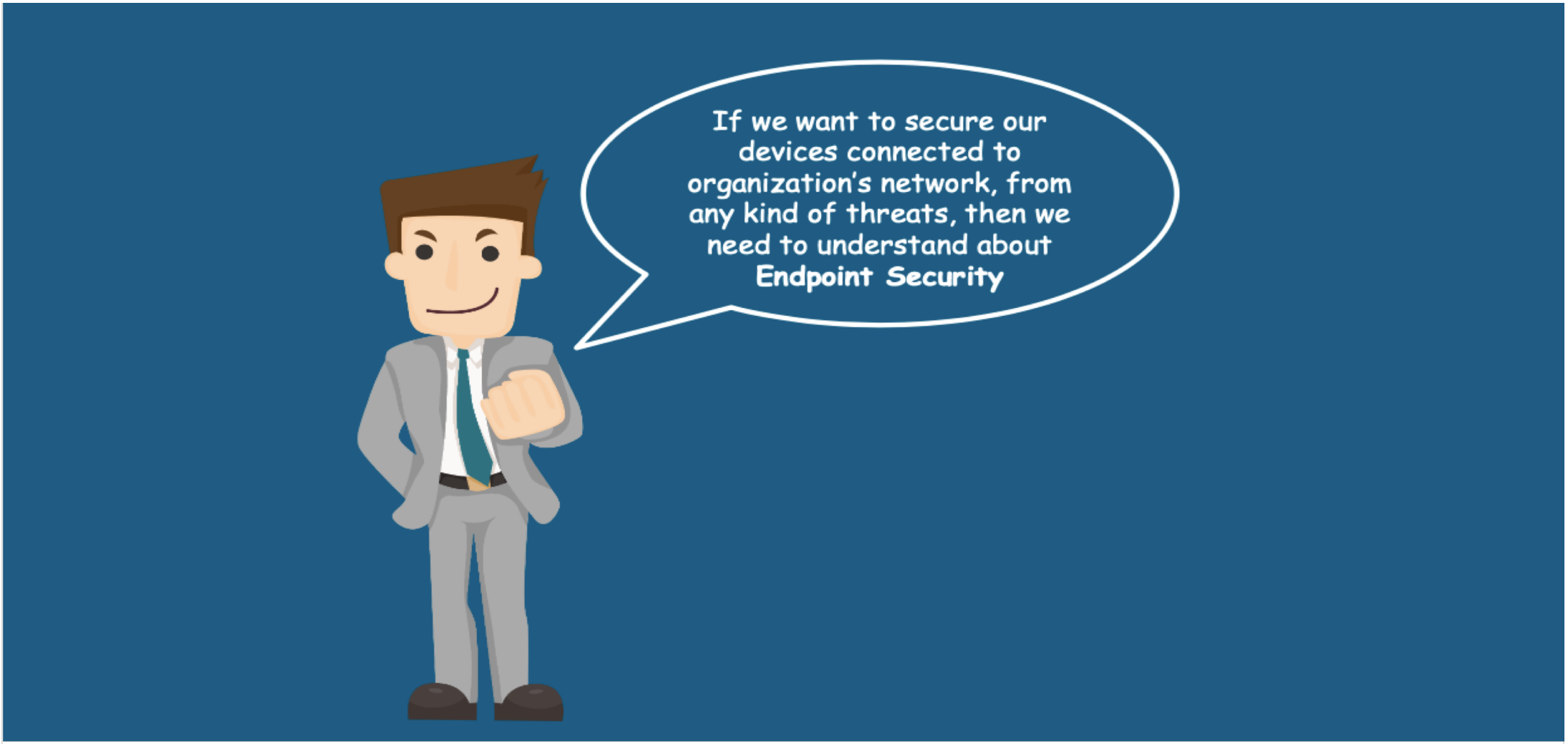
03 Well Managed accounting and control of all devices also helps in planning and executing system backup, incident response, and recovery [BCP/DR]

04 External Hackers are primarily interested in scanning the known address spaces of the target organization - and typically wait for new/weak systems getting attached to the network

05 Internal Hackers (typically insiders such as disgruntled, leaving, experimentalist, notorious employees) are interested in connecting rogue devices into the network to gain unauthorized access for activities such as data stealing, application injection, shadow IT and so on

Standard Recommendations By CIS Top 20 Controls List

- Utilization of an active discovery tool for identification of devices connected to the network and updating of the centralized "asset inventory"
- Maintain an accurate and up-to-date inventory of all technology assets (applications, infrastructure components) carrying potential to store or process information useful for the business
- This inventory is expected to include all hardware & software assets, irrespective of them being connected to the organization's network or NOT


If we want to secure our devices connected to organization's network, from any kind of threats, then we need to understand about Endpoint Security

Endpoint Security

Endpoints

- Any computing device, usually an end-user device connected to the organization's network are termed as "Endpoint"
- Examples of usually seen endpoints in an organization include:
  - PC, laptop, tablets
  - Smart-phones
  - Routers/Wi-Fi
  - POS (Point-of-sale) devices
  - Smart Cameras
  - IoT devices

What Is Endpoint Security?

- Endpoint security is the process of **Preventing Threats** on devices connected to the organization's network
- This is the key because most of organization's classified data & applications reside on authorized endpoints
- Due to diminishing network perimeter & usage of personal devices & **BYOD(Bring Your Own Device)** models for enterprise computing rises the potential of personal devices connecting to corporate network & thus storing & processing company's classified data
- Hence one of the key aspects of Data security after classification & network security is endpoint security, as endpoints are not only the storehouses & processors of data but are closest to human interaction level

Endpoint Security Solutions

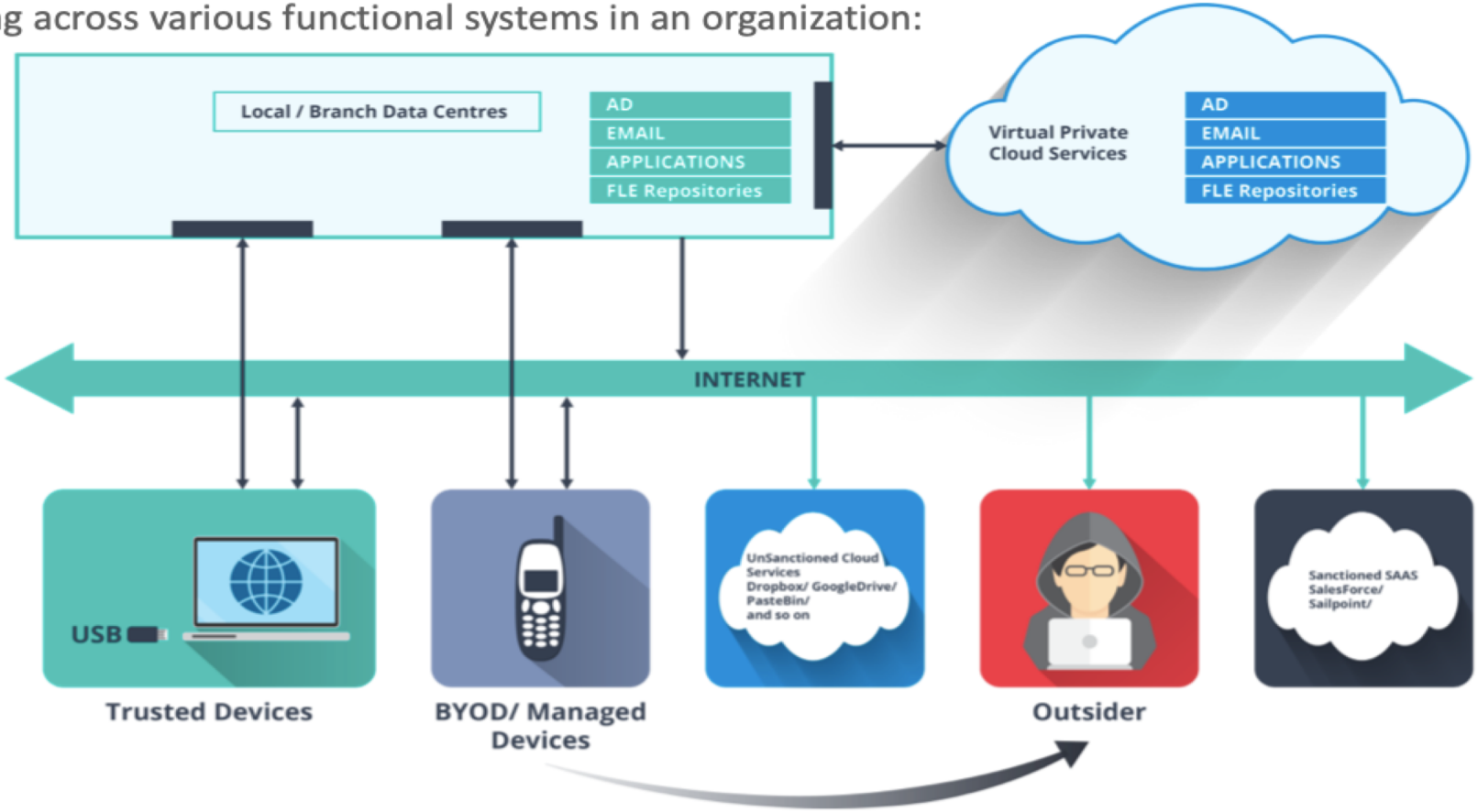
Endpoint security products may contain features & functionality such as:

- DLP (Data loss prevention)
- URL Proxy (Browser level)
- Encryption (Disk level/ email)
- Process monitoring, sandboxing, alerting & response
- Anti-Malware/ Anti-Virus
- Configuration control (Application/ Patches/ OS)
- Network access control
- Data classification & IRM (Information Risk Management)
- Privileged user control

Endpoint Security Risk Scenarios

Typical Enterprise Data Flow Scenario

Data Flowing across various functional systems in an organization:

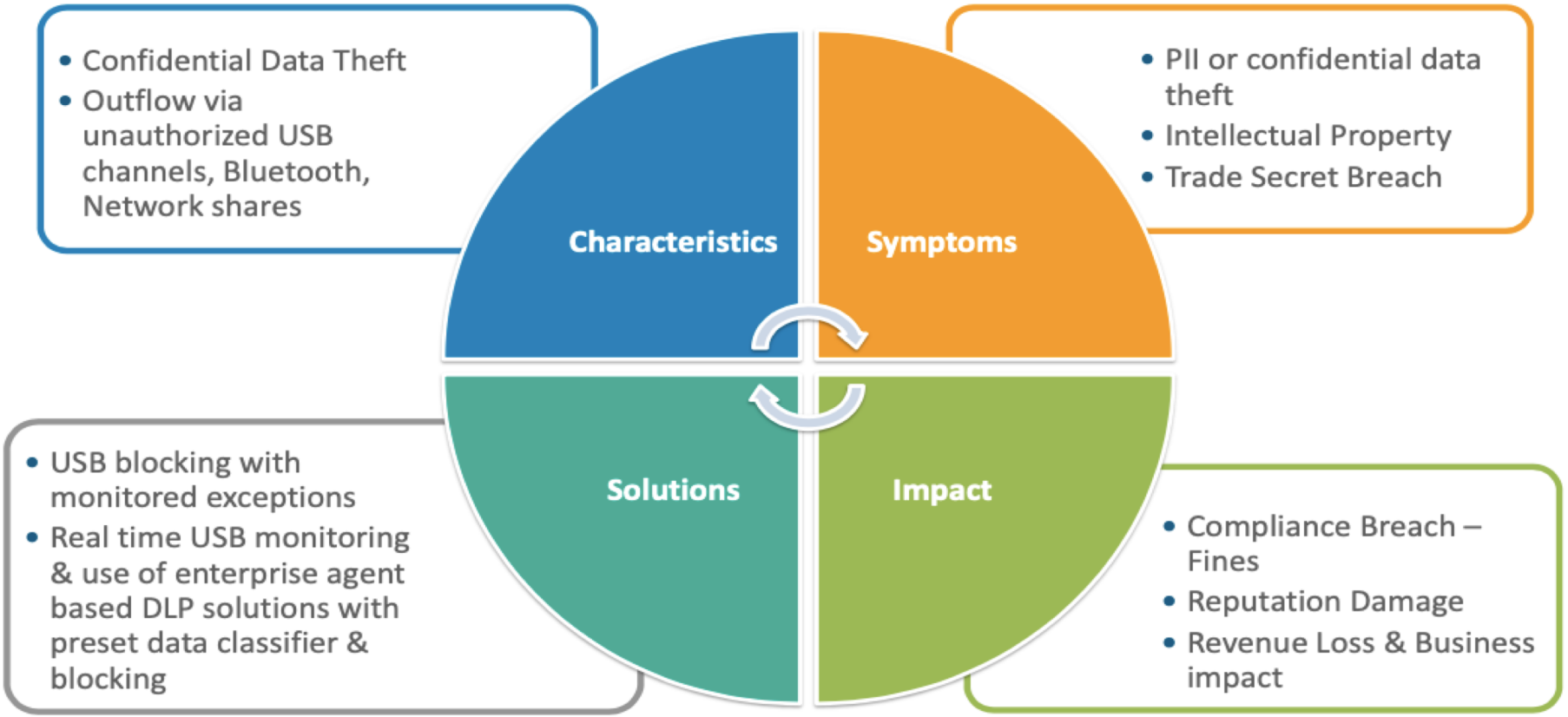


Typical Enterprise Data Flow Scenario – Explanation

- In this data flow scenario we need to Identify the below points:
  - Various data leakage points such as USB, cloud and so on
  - Shadow IT

- **Shadow IT :**
  - Typically a term used to refer the IT services, software components, programs, utilities, cloud – SAAS apps and so on– that are not specifically contracted, whitelisted, authorized or managed by an enterprise. Employees usually get tempted to use such software utilities for getting their jobs done quickly which the available utilities do not provide
  - These are blackspots when it comes to monitoring, incident response and so on

Data Leakage Over Removable Devices

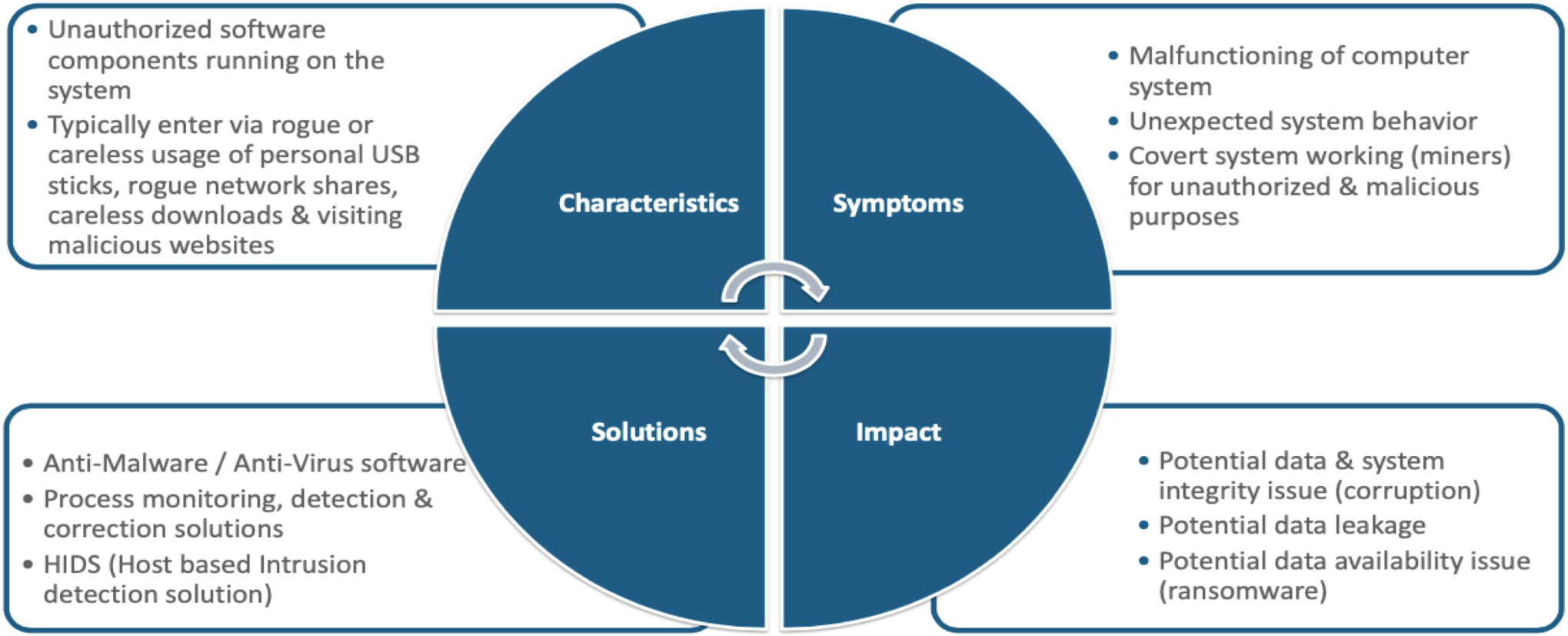


What Is A Malware?

Any software component which behaves in an un-intended, malicious or unauthorized way and effects either of the confidentiality, integrity and availability of the infected system or its components is known as **Malware**

Different Types Of Malware

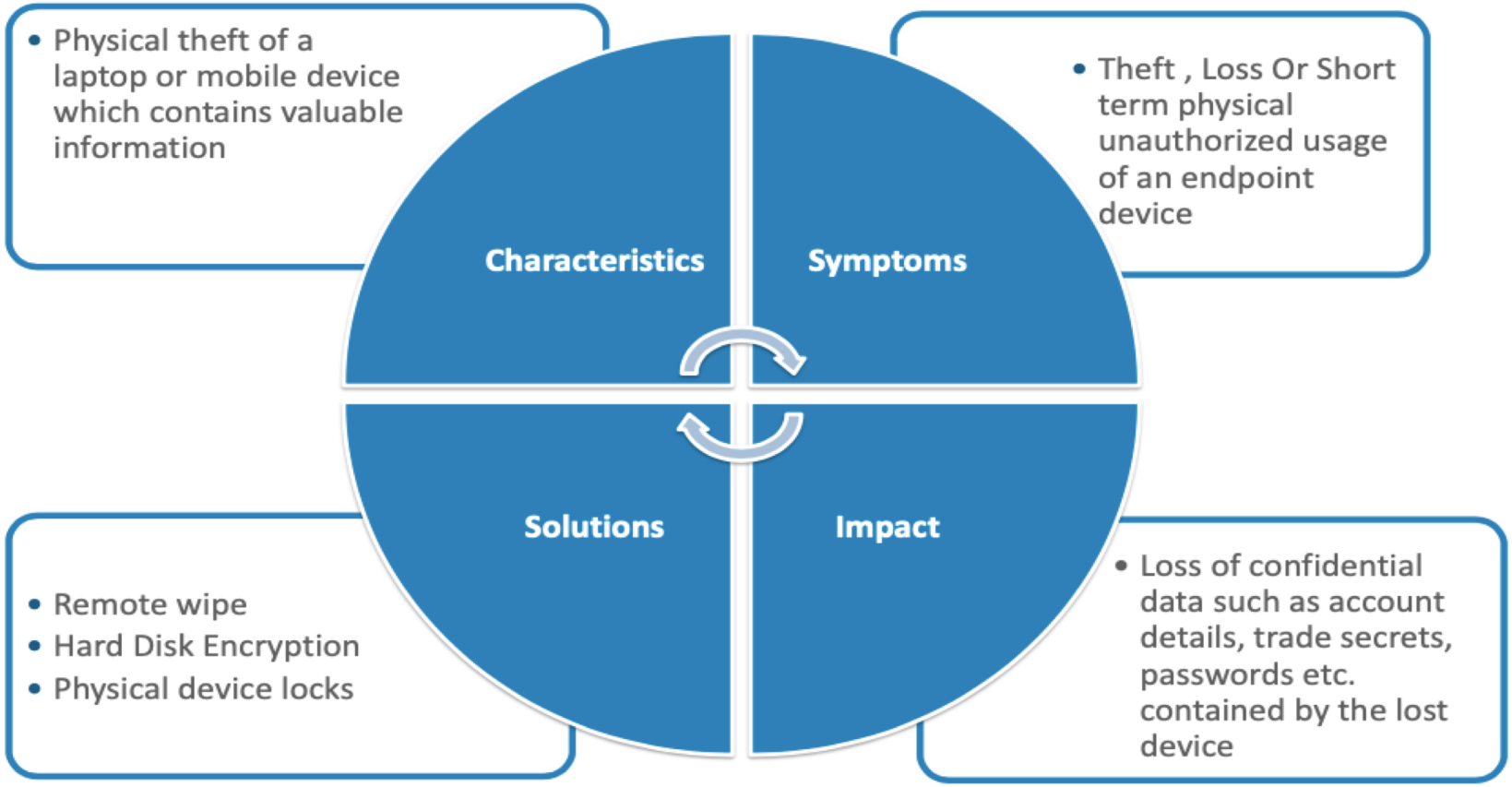
Malware – Features



What Is Endpoint Device Theft?

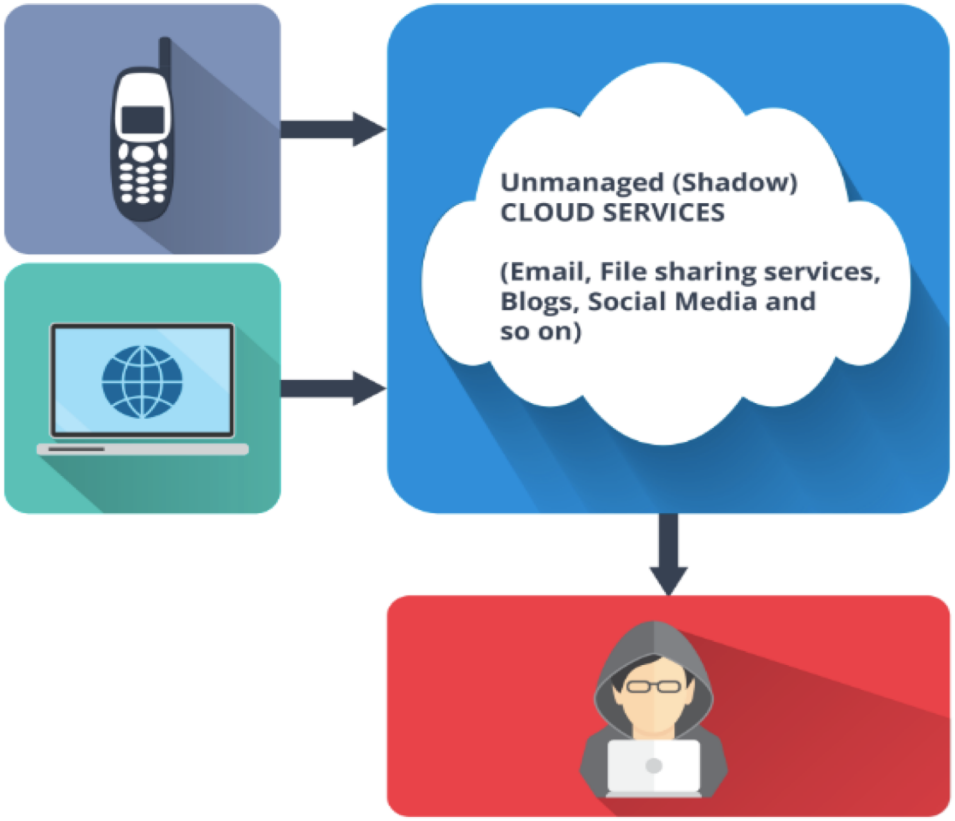
- Endpoint Device theft includes theft of any device such as mobile phones, computers, laptops, tablets and so on
- Apart from device cost, the devices contain lot of confidential data, which comes at risk

Endpoint Device Theft

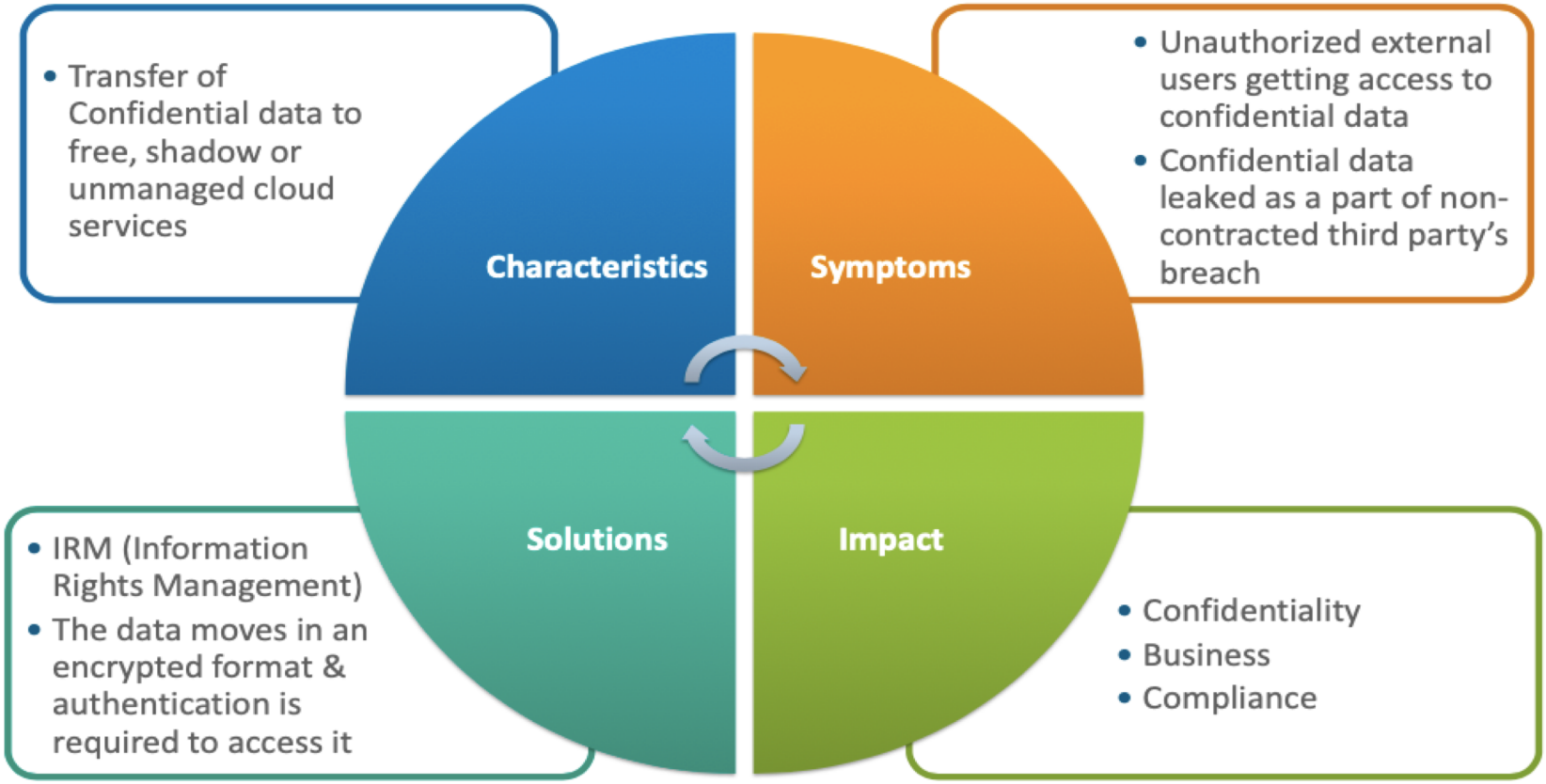


What Is Data Leakage Over Cloud?

Data being sent by endpoints to unauthorized cloud services which eventually get hacked by external attackers and the confidential data gets leaked

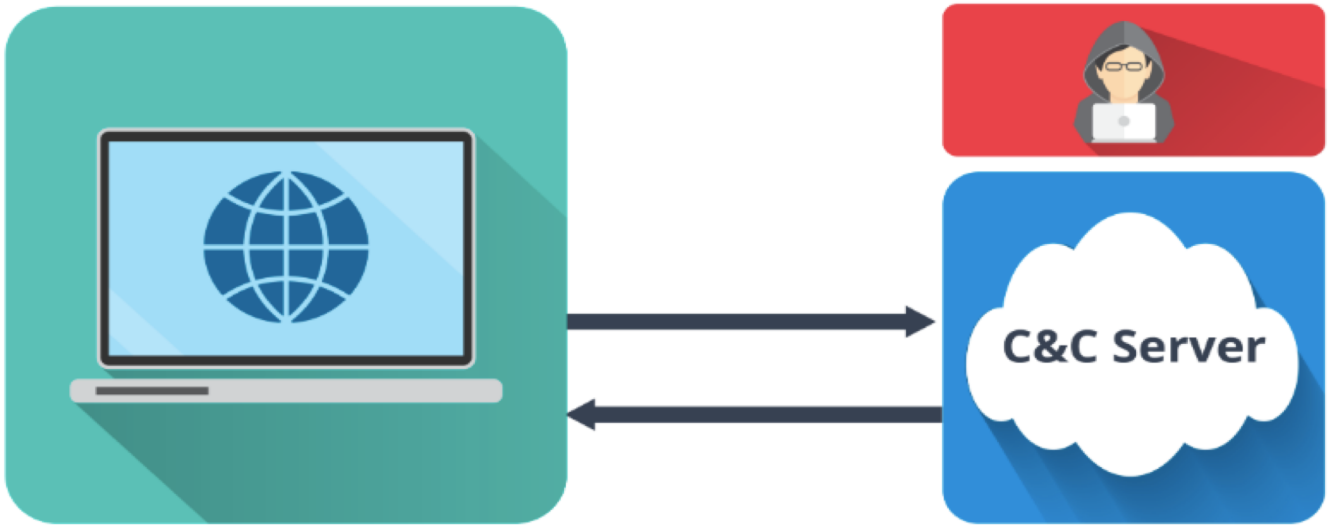


Data Leakage Over Cloud

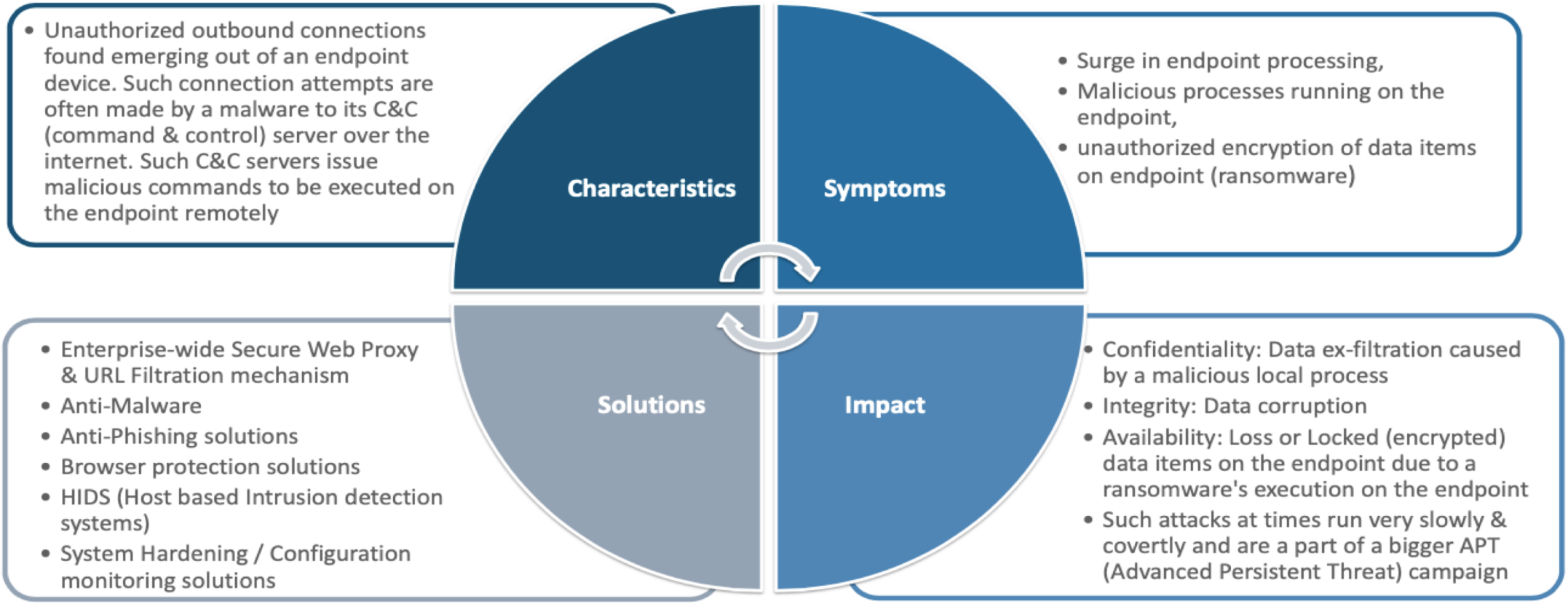


What Is Unauthorized Browsing?

- **Endpoint** establishes unauthorized connections with servers set up by Hackers (usually referred to as C&C servers)
- **C&C (Command and Control)** servers are centralized servers that are able to send commands and receive outputs of devices, typically part of a botnet
- Attackers wishing to launch a **DDoS (Distributed Denial of Service)** attack may just send a few special commands to the associated C&C servers of their botnet, with instructions to perform an attack on a particular target. The infected devices communicating with the contacted C&C server will obey by launching a corresponding coordinated attack



Unauthorized Browsing



- Unauthorized outbound connections found emerging out of an endpoint device. Such connection attempts are often made by a malware to its C&C (command & control) server over the internet. Such C&C servers issue malicious commands to be executed on the endpoint remotely

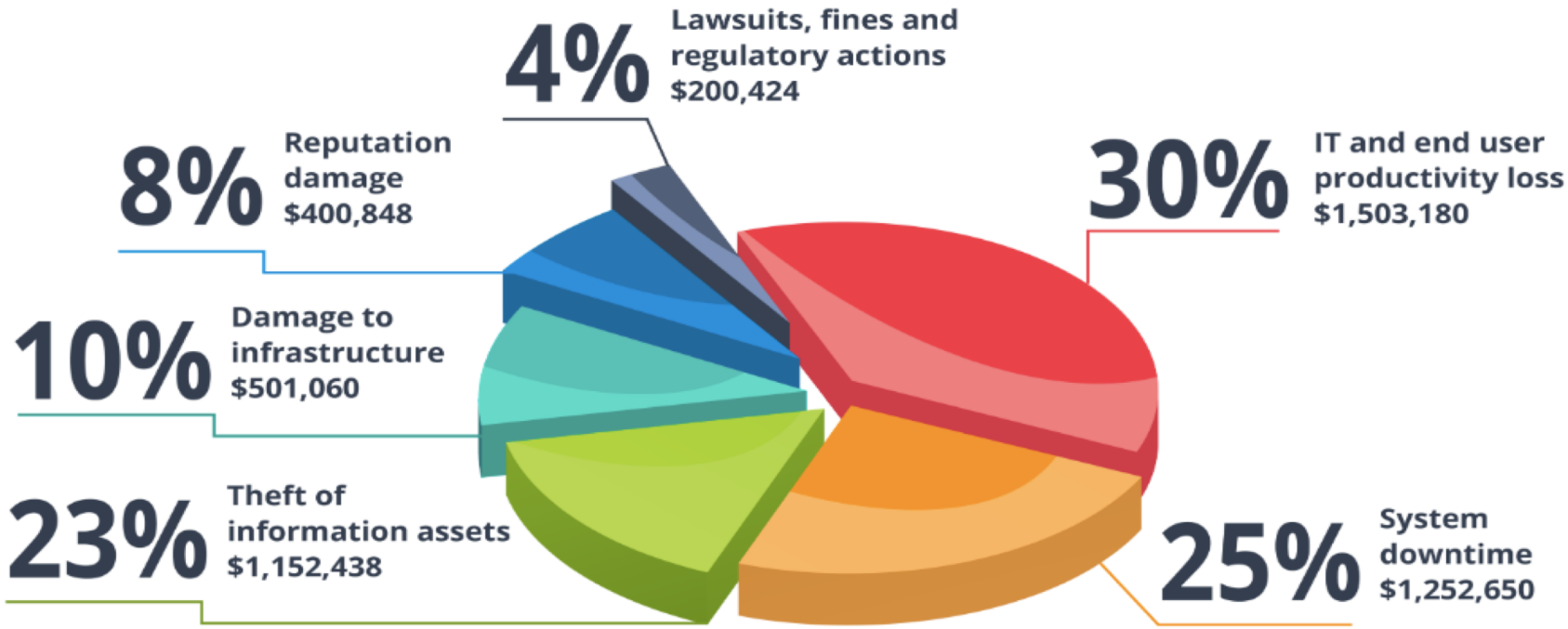
- Surge in endpoint processing,
- Malicious processes running on the endpoint,
- unauthorized encryption of data items on endpoint (ransomware)

- Enterprise-wide Secure Web Proxy & URL Filtration mechanism
- Anti-Malware
- Anti-Phishing solutions
- Browser protection solutions
- HIDS (Host based Intrusion detection systems)
- System Hardening / Configuration monitoring solutions

- Confidentiality: Data ex-filtration caused by a malicious local process
- Integrity: Data corruption
- Availability: Loss or Locked (encrypted) data items on the endpoint due to a ransomware's execution on the endpoint
- Such attacks at times run very slowly & covertly and are a part of a bigger APT (Advanced Persistent Threat) campaign

Cost Distribution Of Endpoint Attacks

2017 Survey results published by Ponemon Institute (a renowned research center on the subject of data privacy and protection)



Source: https://www.ponemon.org/blog/the-2017-state-of-endpoint-security-risk-report

Endpoint Monitoring and Management Solutions

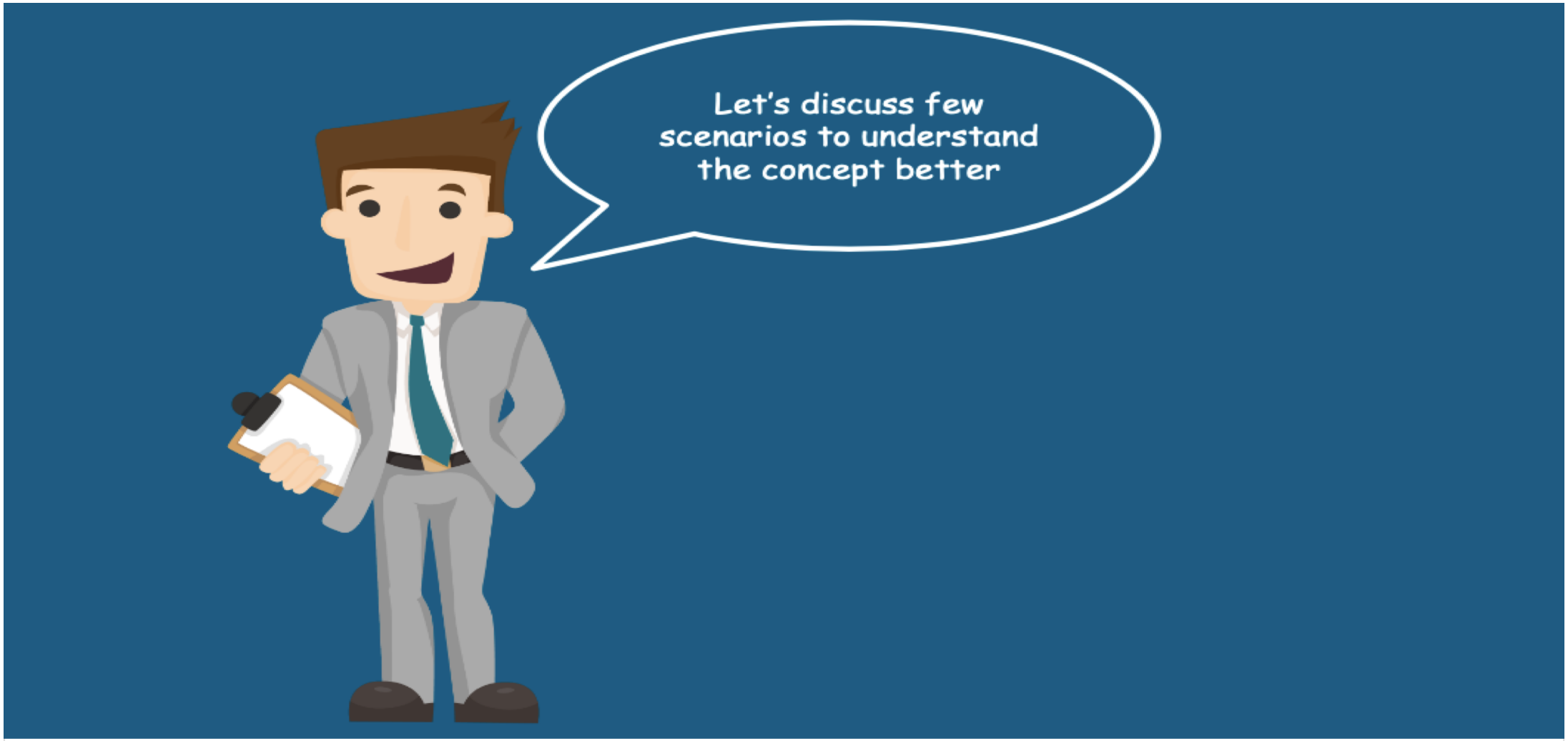
Modern Inclusive Endpoint security solutions help in centralized enforcement of security policies, ensuring proper controls are in place & minimizing erroneous misconfiguration

They also help to achieve key activities:

- Provision virtual systems or deploy software
- Patch operating systems and applications
- Inventory hardware and software assets
- Monitor software and licensing usage
- Manage configurations on the go
- Manage reimaging, re-deployments and decommissioning of assets
- Help remote monitoring & controlling the processes on the endpoints
- Detect, Block & Alert on malicious processes - Signature (IOC : Indicator of compromise), Heuristic & Machine learning based
- Help in remote memory imaging & other digital forensic requirements
- Implements Deception for early detection of threats

Apart from Malware detection & response, these tools can help organizations in :

- Set a security baseline,
- Ensure minimal & accepted drift from established standards (exceptions)
- Control and manage automatic updates
- Protect against user-induced errors
- Block unauthorized configuration changes
- Discover assets


Let's discuss few scenarios to understand the concept better

Scenario 1 – Discussion

Consider modern endpoints (laptops, mobile phones, tablets) which keep moving in & out of managed corporate network & travel across various geo-locations

Consider ease of browsing, personal data processing on enterprise endpoints

As 'Freedom comes with lots of responsibility' - all this freedom of usage of enterprise endpoints brings in lots of risks

Scenario 2 – Discussion

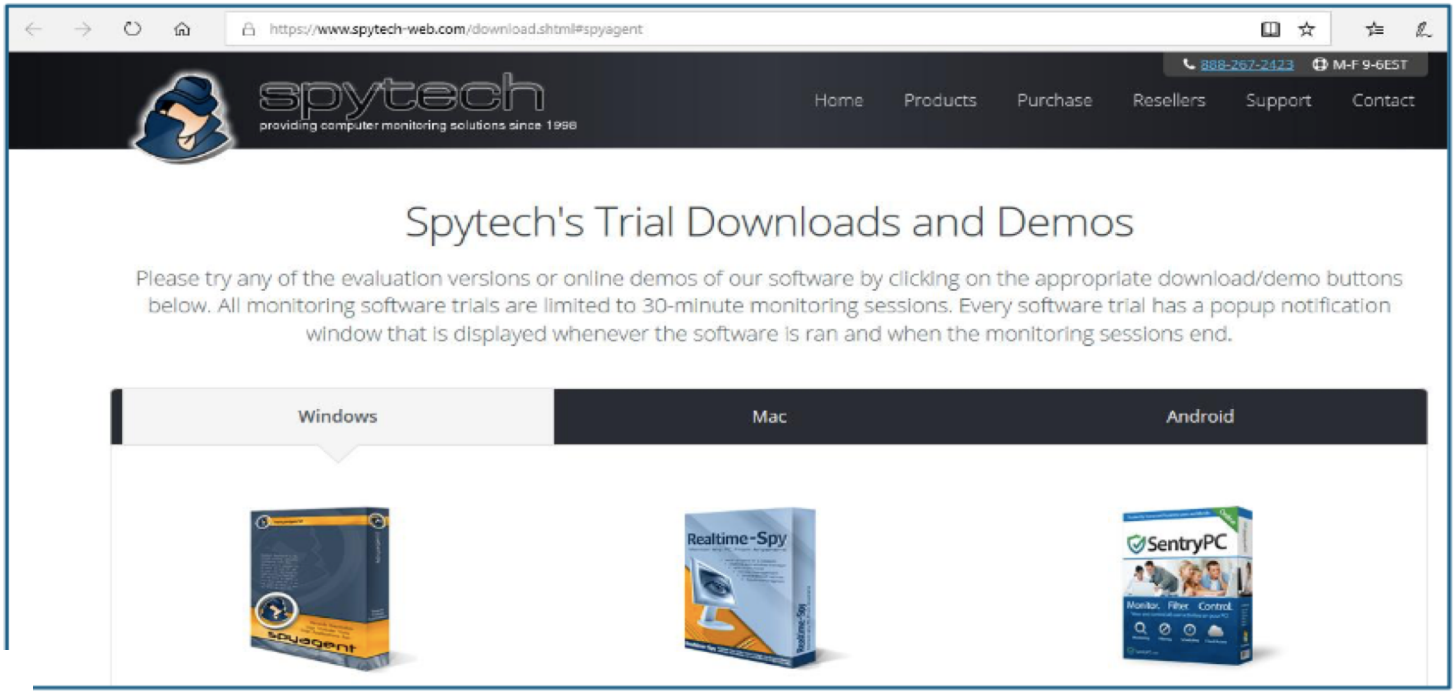
Consider BYOD (Bring Your Own Device) – for ease of use & enterprise cost shift

Consider having personal data & enterprise confidential data on the same device in parallel

As 'Freedom comes with lots of responsibility' - all this freedom of usage of enterprise endpoints brings in lots of risks.

Demo 1: Computer Monitoring

- Monitor the users activities on your system stealthily
- Install and configure **SpytechSpyagent** from the following location: https://www.spytech-web.com/download.shtml#spyagent



Demo 2: System Recovery

- Recover the system in case of system failure
- Creating restore points and recovery disc in order to recover system

Proposed Endpoint Security Maturity Model (SANS)

FTVETI

ICT @ FTVETI

Endpoint Security – SANS Endpoint Maturity Model

- **Maturity Model:** Best way to control and make efficient usage of an ever increasing "endpoint diversity" is to wrap servers, mobile devices, kiosks, HVAC, industrial systems, cameras and even automobiles into a endpoint security
- Based on the reasonable grounds, lower security maturity represents higher risk in this model
- This model is great for evaluating an enterprise's endpoint security levels, it is too broad for use as a "focused tool" at the endpoint

Source: https://www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342

Maturity Levels – SANS EP Maturity Model

- Such a model is helpful in evaluating the current status of endpoint security for an organization and also helps itself to benchmark its processes with other peer organizations, thus strategize its plan of action towards next maturing stage
- Evaluation of maturity & benchmarking forms a standard industry best practice and helps in maintaining organization's focus towards a specific process, periodic reviews & progress tracking

Level 1	Level 2	Level 3	Level 4	Level 5
Random or Disorganized The Level 1 organization is a disaster waiting to happen, but like the Titanic, it moves ahead, blissfully unaware of the danger that endpoints are already leaking	**Reactive or Tactical** Level 2 organizations pay lip service to endpoint security, but their actions are woefully insufficient to protect against any but the most amateur attacker	**Preventative** Level 3 organizations possess a false sense of security that their endpoint compliance programs represent sufficient obstacles for determined attackers	**Organized or Directed** Level 4 organizations have their acts together and may represent a peak state for many organizations. But they still need complete commitment to endpoint security from top management to advance Level 5	**Proactive, Comprehensive, Continuous and Measurable** Level 5 organizations nurture a culture of security, wherein all employees consider security to be part of their job

Source: https://www.sans.org/reading-room/whitepapers/analyst/curve-maturity-model-endpoint-security-36342

Quiz #1

- The primary security risk for an organization, on an event of theft or loss of a device is?
  a. Confidentiality
  b. Availability
  c. Authenticity
  d. Integrity

Answer #1

- The primary security risk for an organization, on an event of theft or loss of a device is?
  a. **Confidentiality**
  b. Availability
  c. Authenticity
  d. Integrity

Answer a:
Explanation: Enterprises issue endpoints and devices for storing, processing & transferring it's data, most of which could be confidential or sensitive in nature. Loss and Theft of a device could potentially increase the chances of sensitive data leakage to unauthorized parties. Hence Confidentiality is the key

Quiz #2

- What is the first step towards defining an organization's data security strategy?
  a. Designing Data Security Controls for all business functions
  b. Creating a overall Risk Mitigation plan for security incidents
  c. Defining Organization-wide Data Classification scheme
  d. Creating a Data Backup & Recovery Plan

Answer #2

- What is the first step towards defining an organization's data security strategy?
  a. Designing Data Security Controls for all business functions
  b. Creating a overall Risk Mitigation plan for security incidents
  c. **Defining Organization-wide Data Classification scheme**
  d. Creating a Data Backup & Recovery Plan

Answer c:
Explanation: Data classification is an important process of segregating data into various categories so as to ensure its effective and efficient usage through it's lifecycle. Data Classification is the basis of Data security strategy as the classification levels guide further process of prioritization of data security aspects, methods of data handling, security control selection, data retention and so on

Quiz #3

- One of the most effective technical control to centrally secure access to confidential data files, while on the move across devices, cloud platforms & users (internal, external, vendors and so on) is?
  a. DLP (Data Leakage Prevention)
  b. IRM (Information Rights Management)
  c. Network Firewall
  d. Next Gen Anti-Virus

Answer #3

- One of the most effective technical control to centrally secure access to confidential data files, while on the move across devices, cloud platforms & users (internal, external, vendors and so on) is?
  a. DLP (Data Leakage Prevention)
  b. IRM (Information Rights Management)
  c. Network Firewall
  d. Next Gen Anti-Virus

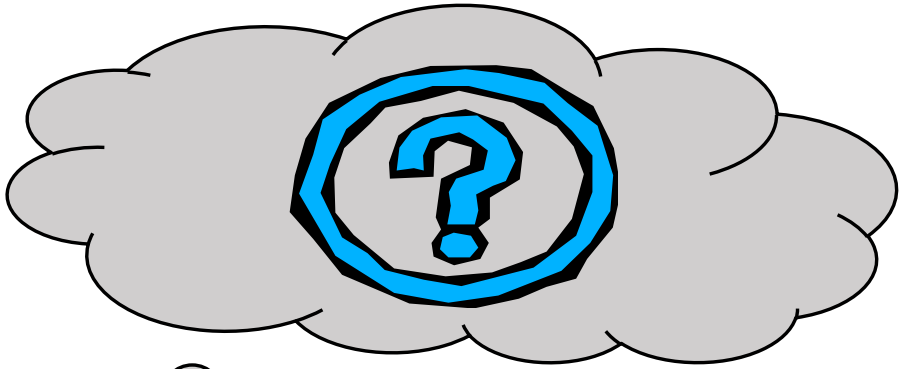
Answer b:
Explanation: Information Rights Management (IRM) is a special security technology often used to protect sensitive information from unauthorized access. IRM applies to files, office documents, presentations, spreadsheets and so on, created by internal users or employees. IRM technology typically encrypts the document & attaches a security label to it, thus enabling only the authorized parties being able to gain access to the documents. Such level of access is usually controllable centrally. Hence such protected data files can move across boundaries without fear of potential data leakage to unauthorized users and parties

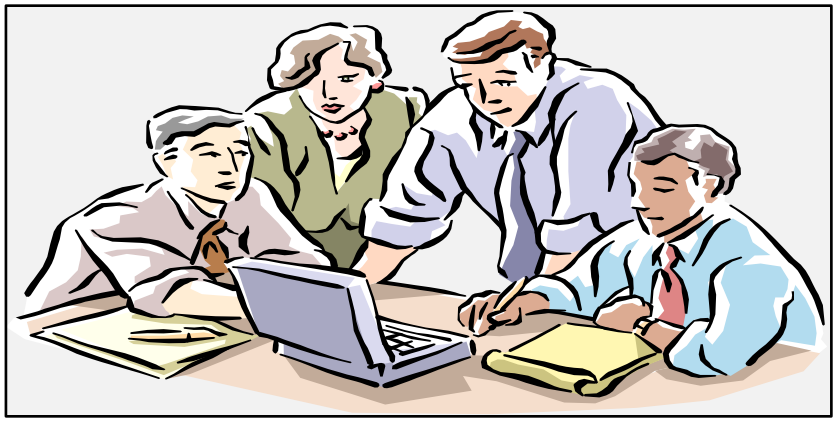
Summary

In this unit, you should have learnt:

- Data Classification principles
- The need of Maintenance of an Asset inventory from information security perspective
- Computing Endpoints
- Endpoint Security risks & controls
- SANS Endpoint Security Maturity Model
- Feature of today's comprehensive endpoint security solutions

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI