Co-funded by the European Union

Course: Real time Cyber Threat Detection and Mitigation

Project: Cyber Security 4 ALL(CS4ALL)

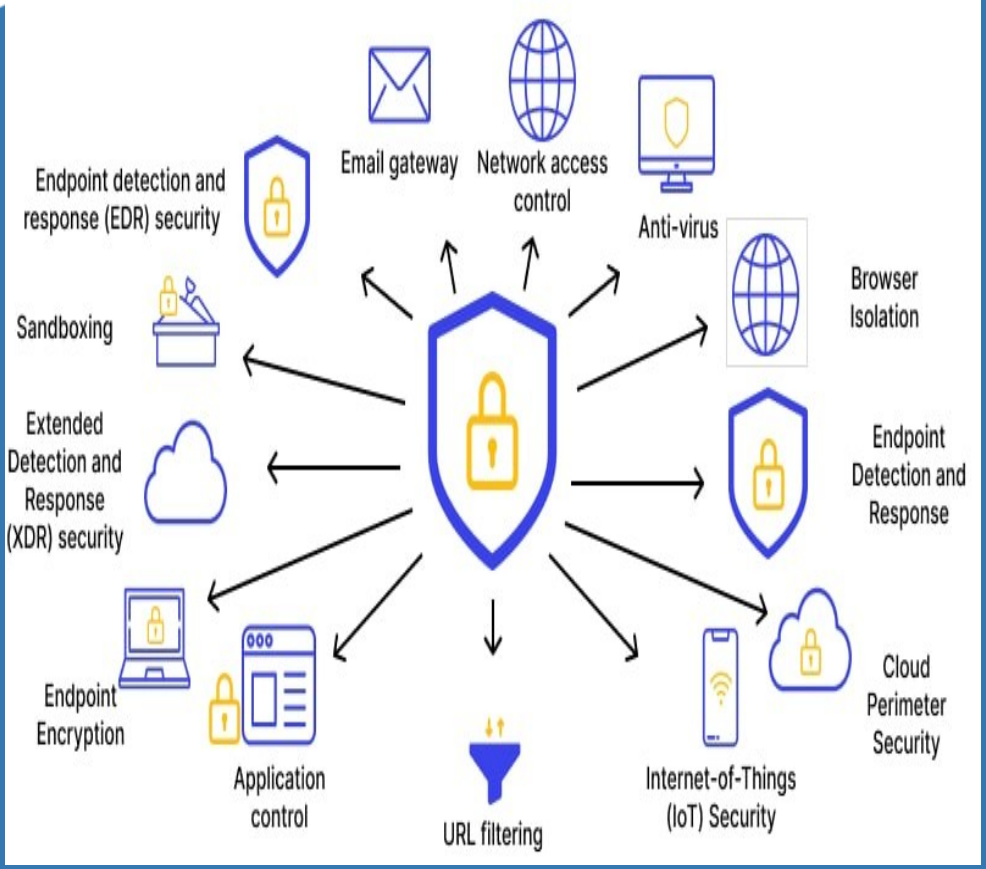
Co-funded by
the European Union

Chapter 5
Endpoint Protection

INDEX

Co-funded by
the European Union

Overview



- In today's rapidly evolving cybersecurity landscape it is crucial to
  - protect endpoint devices—such as desktops, laptops, and mobile device
  - safeguard sensitive data
  - ensure the integrity of enterprise networks
- Endpoint protection
  - a multilayered approach, utilizing various tools and techniques to prevent, detect, and respond to security threats.

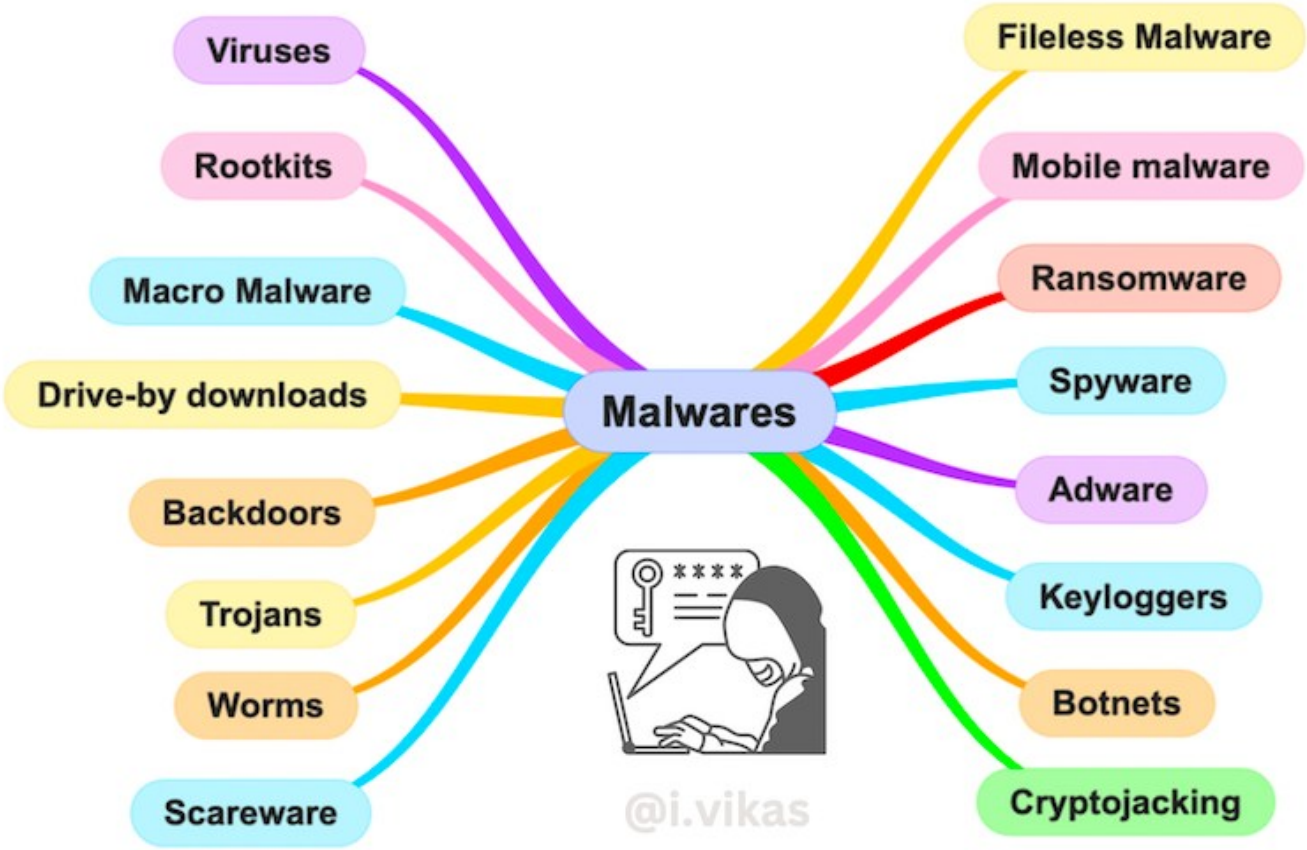
What is Malware

- Software designed to damage, disrupt, or steal data from systems.
- Forms include viruses, trojans, ransomware, and spyware.
- Spreads via email, downloads, or compromised websites.
- Goals include data theft, system damage, or control
- Prevention includes antivirus tools, updates, and safe online practices.

Co-funded by the European Union

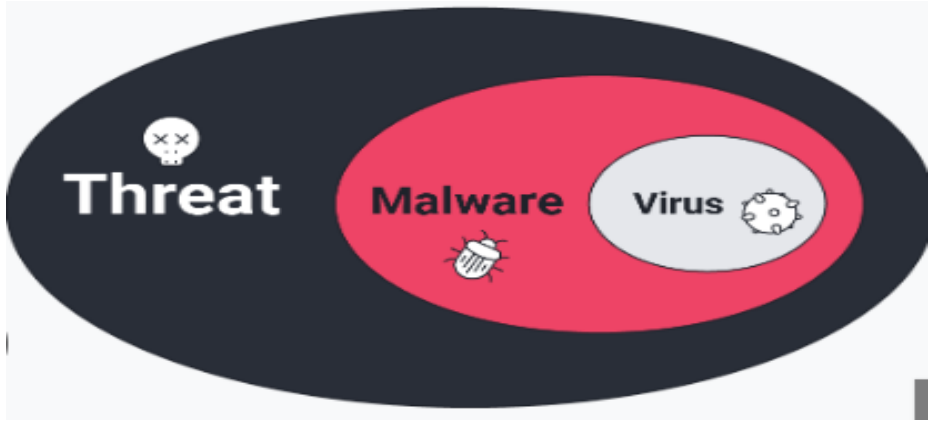
Co-funded by
the European Union

Types of Malware



What is Virus

- Specific type of malware
- Attaches itself to legitimate files
- Spreads from one system to another
- Requires user interaction to propogate
- Cause range of harmful effects



Co-funded by
the European Union

Co-funded by
the European Union

Types of Virus

- File Infector Viruses
- Macro Viruses
- Boot Sector Viruses
- Polymorphic Viruses
- Metamorphic Viruses
- Resident Viruses
- NonResident Viruses
- Multipartite Viruses
- Trojan Horses (Trojan Viruses)
- Rootkits
- Resident Boot Sector Viruses

Co-funded by
the European Union

Impact of Malware

1. Data Theft and Privacy Breaches
2. Financial Fraud
3. System and Network Damage
4. Disruption of Operations
5. Increased Security Vulnerabilities
6. Reputation Damage
7. Legal and Regulatory Consequences
8. Resource Drain

Co-funded by
the European Union

Impact of Viruses

1. Data Corruption
2. System Disruption
3. Data Loss
4. Spread to Other Systems
5. Financial Loss
6. Reputation Damage

Endpoint Protection

- Secures network connected devices from threats and vulnerabilities.
- Involves multiple layers of security technologies and practices.
- The goal is to provide a comprehensive defense strategy for endpoint devices.

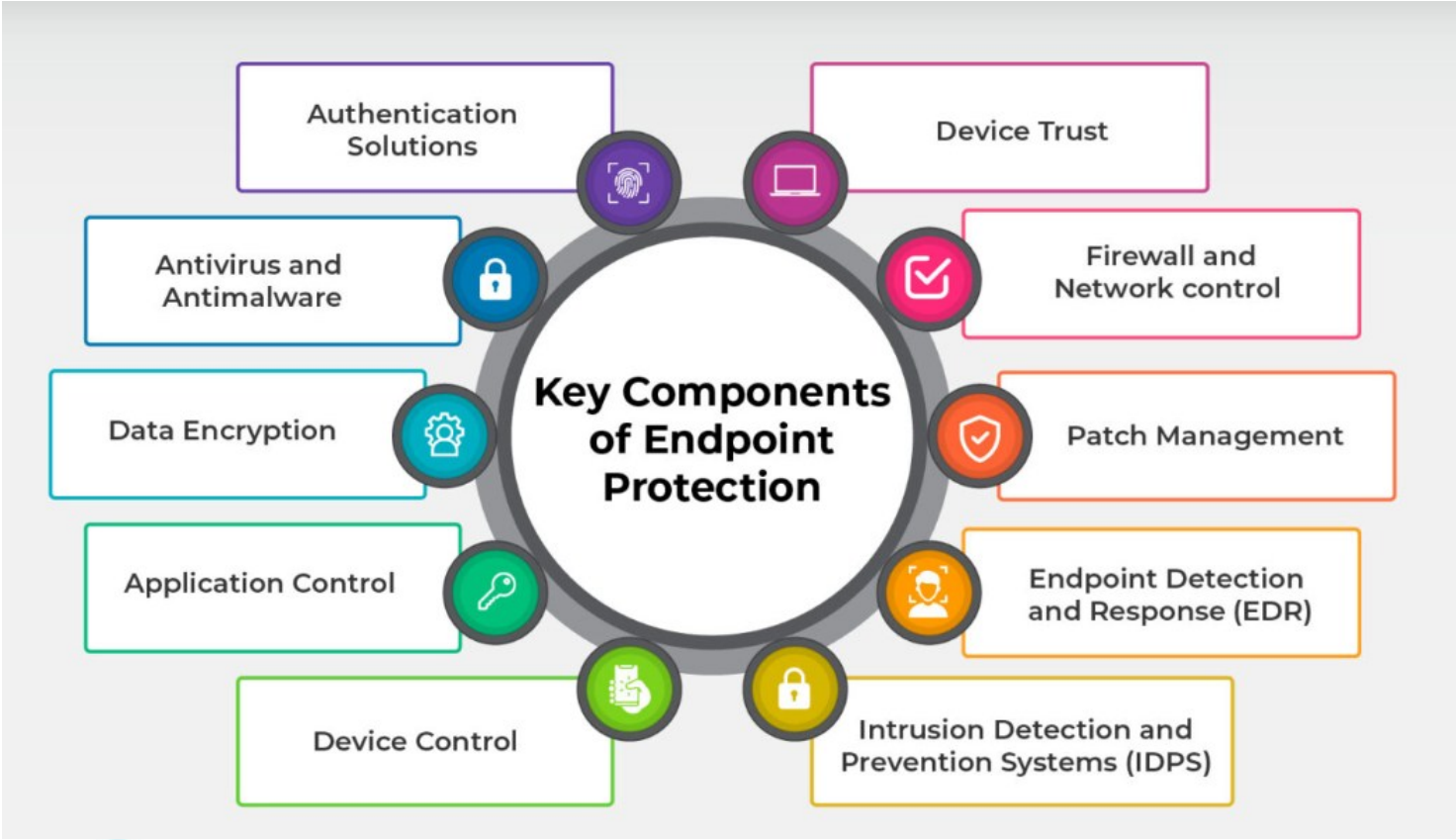
Co-funded by
the European Union

Key Components of Endpoint Protection

1. Antivirus Software
2. AntiMalware Software
3. Firewalls
4. Intrusion Detection and Prevention Systems (IDPS)
5. Data Encryption
6. Endpoint Detection and Response (EDR)
7. Application Control and Whitelisting
8. Patch Management

Co-funded by the European Union

Key Components of Endpoint Protection



Co-funded by the European Union

Why Endpoint Protection is Important

1. Attack Surface Reduction
2. Prevention of Data Breaches
3. Operational Continuity
4. Threat Mitigation

Co-funded by the European Union

5.1 Antivirus

Type of security program designed to detect, prevent, and remove malicious software (malware) from a computer or device.

Focused on protecting systems from viruses and broader range of threats

Key Functions of Antivirus Software

1. Detection
2. Prevention
3. Removal
4. Updates
5. Additional Features

Co-funded by
the European Union

AntiMalware

- Designed to detect, prevent, and remove a broad range of malicious softwares
- various types of threats, including spyware, adware, ransomware, trojans

Key Functions of AntiMalware Software

1. Comprehensive Threat Detection
2. RealTime Protection
3. Removal and Cleaning
4. Updates and Threat Intelligence

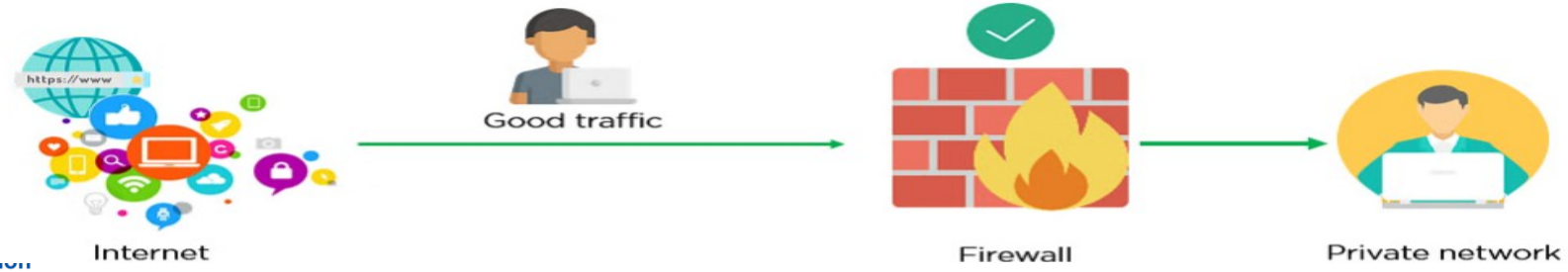
CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

5.2 Firewall Protection

- Monitors and controls network traffic
- Creating a barrier between trusted and untrusted networks.
- Secure individual devices within a network, focusing on computers, servers, and mobile devices.

Key Functions of a Firewall

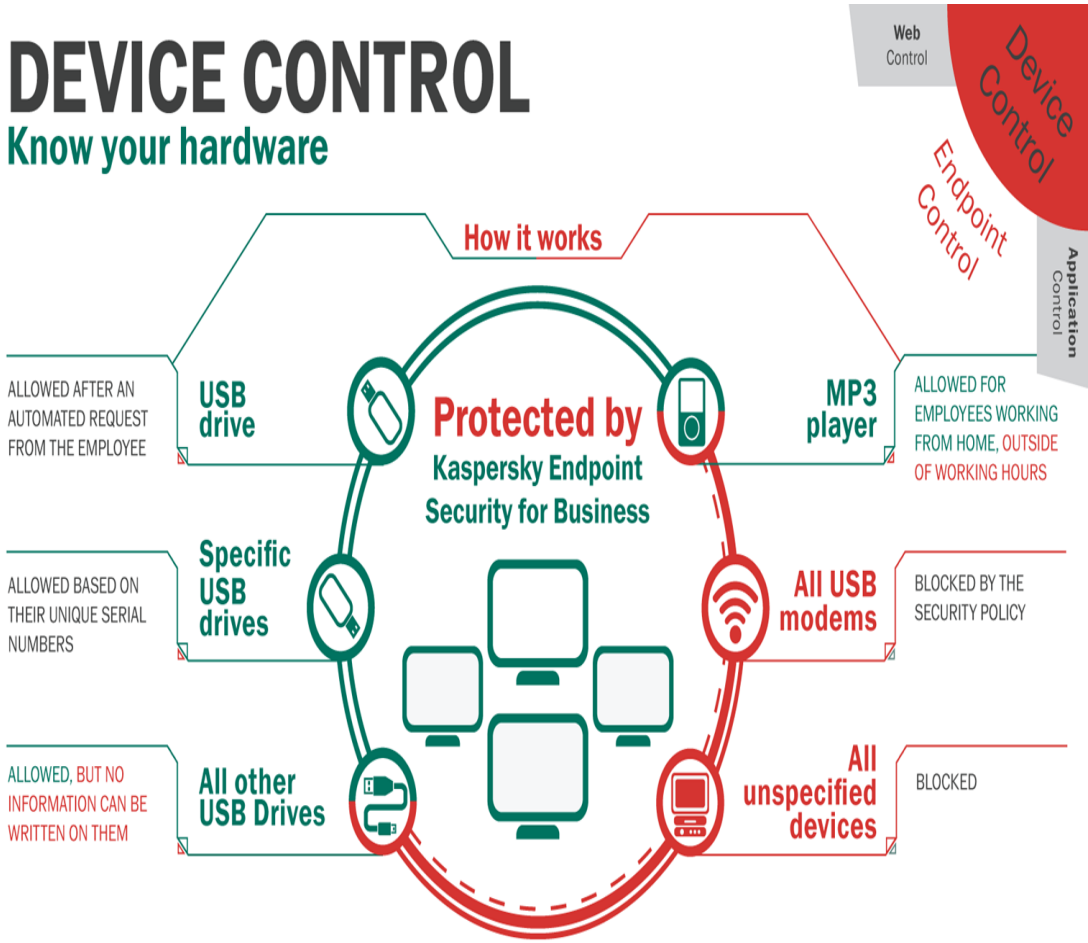
1. Traffic Filtering
2. Access Control
3. Network Segmentation
4. Logging and Monitoring
5. Threat Prevention



Co-funded by the European U...

5.3 Device Control

- Manages access to external devices on network endpoints.
- Regulates USB drives, printers, and other peripherals connected to computers.
- Prevents malware infections, data breaches, and unauthorized transfers.
- Crucial in endpoint protection for safeguarding systems and data.



Co-funded by the European Union

Key Functions of Device Control

1. Device Access Management

Whitelist/Blacklist Devices

Control Device Types

2. Data Transfer Control

Read/Write Restrictions

File and Data Management

3. Monitoring and Logging

Activity Monitoring

Alerts

4. Policy Enforcement

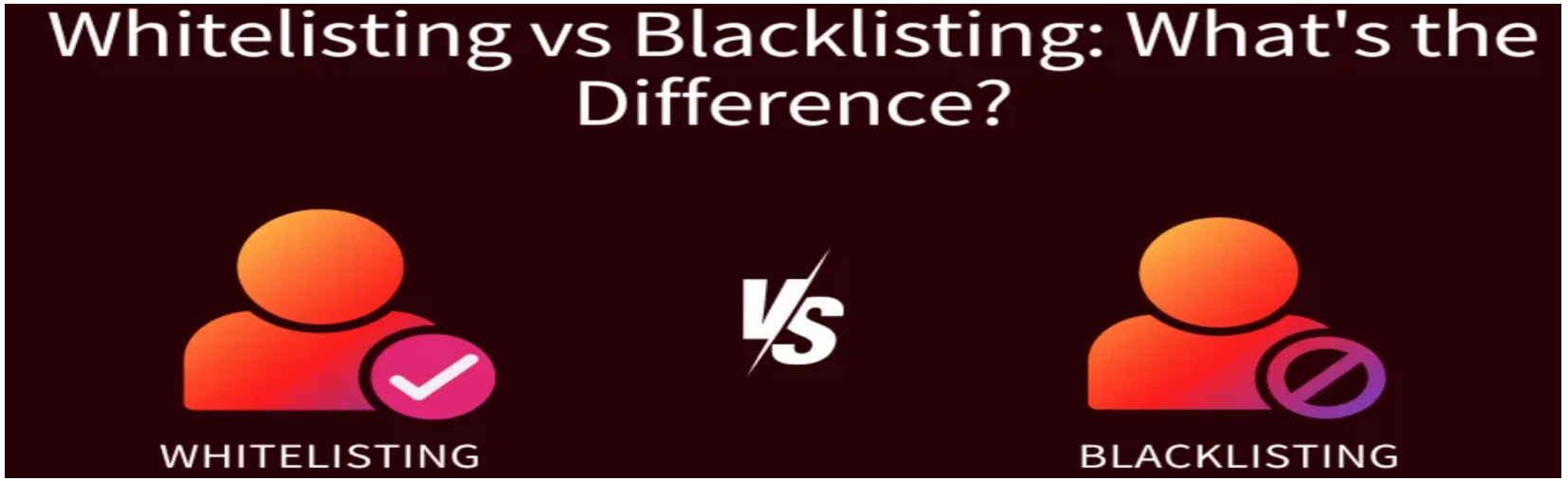
Automated Policies

UserLevel Policies

Co-funded by
the European Union

5.4 Application whitelisting and blacklisting

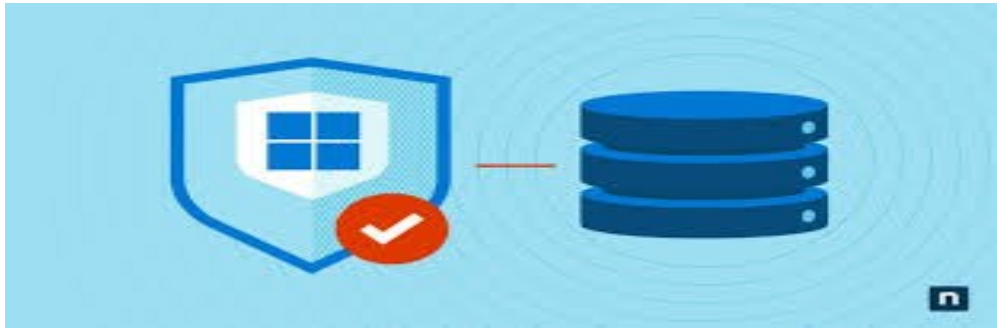
- Designed to safeguard devices like laptops, desktops, and mobile devices from malicious or unauthorized software
- Aims to prevent security breaches and protect sensitive data



Co-funded by the European Union

Application Whitelisting in Endpoint Protection

- Allows only approved, trusted applications to run on devices.
- All other applications are blocked by default.
- Prevents malware and unauthorized software from executing.
- Ensures only known, safe applications are permitted on endpoint devices.

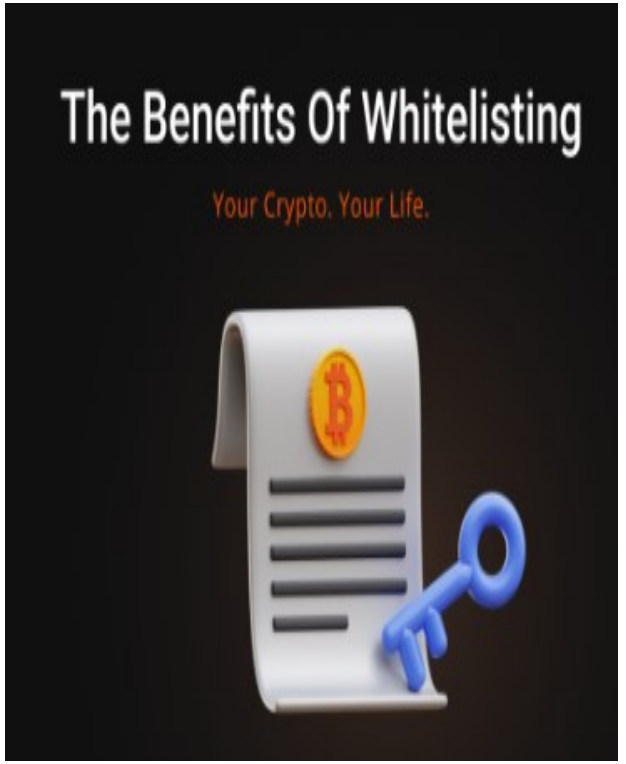


Co-funded by the European Union

Co-funded by
the European Union

Advantages Of Whitelisting

- **High Security**
- **Control**
- **Compliance**



Co-funded by
the European Union

Challenges Of Whitelisting

- **Maintenance**
- **Flexibility**

Application blacklisting in Endpoint Protection

- **blocks known malicious or unwanted applications**.
- **All other applications** are allowed unless blacklisted
- Prevents execution of **explicitly identified harmful software**.
- **Opposite of whitelisting**, where only approved apps can run.

Co-funded by the European Union

Co-funded by
the European Union

Advantages Of Blacklisting

- Simplicity
- User Flexibility

Co-funded by
the European Union

Challenges Of Blacklisting

- Less Secure
- Reactive Approach

Use Cases in Endpoint Protection

1. Highly Secure Environments

2. General Corporate Environments

3. Dynamic Environments

Co-funded by
the European Union

5.5 Patch Management

- The process of applying updates to software, drivers, and firmware to protect against vulnerabilities
- Ensure the best operating performance of systems, boosting productivity

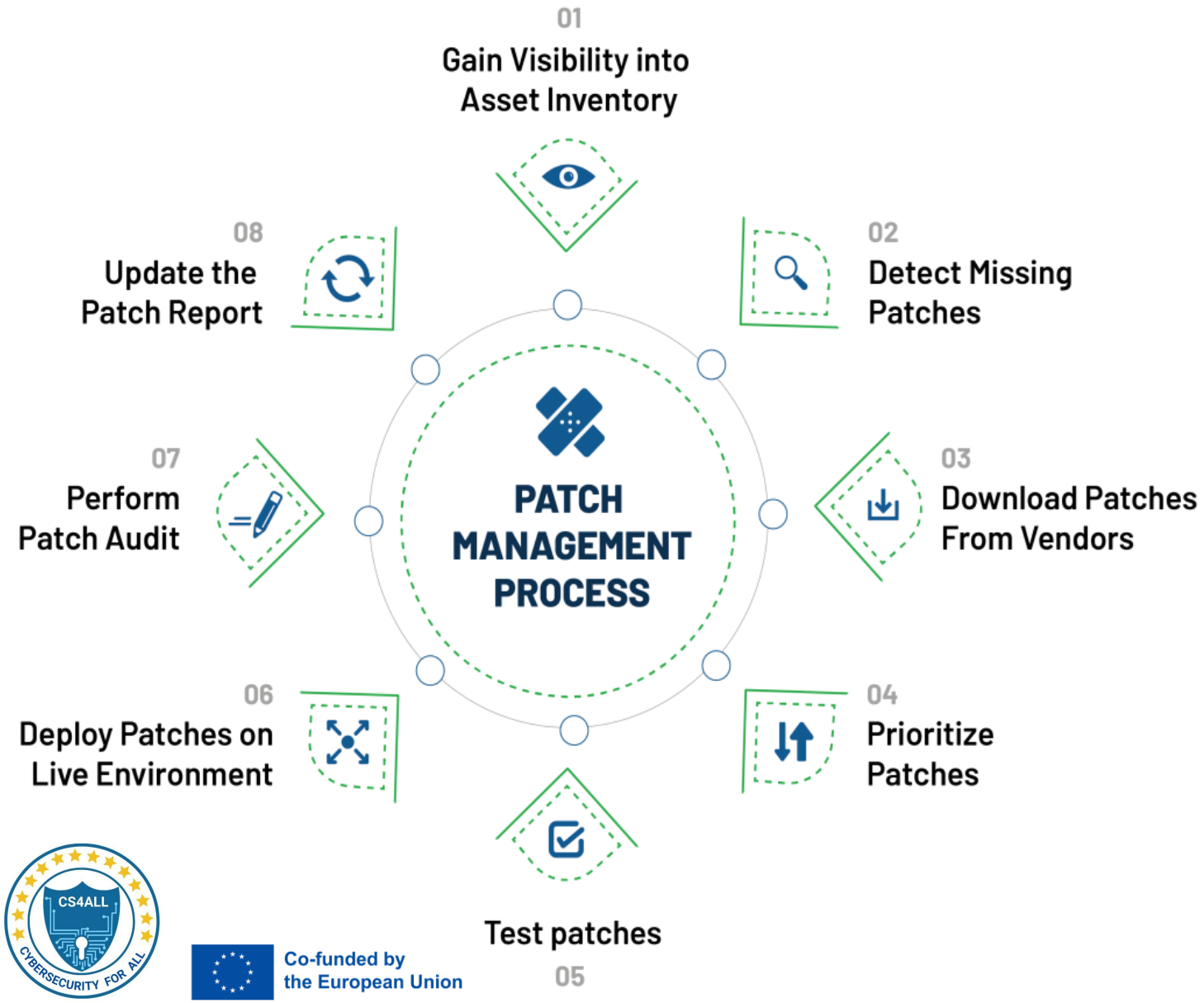
Co-funded by
the European Union

Why is Patch Management Important?

- Need of patching is exploding as 5G networks
- The rise of AI is providing hackers with new tools for penetrating networks
- Keep computers and networks secure, reliable and up to date
- Improves performance

Co-funded by the European Union

How does Patch Management Works ?



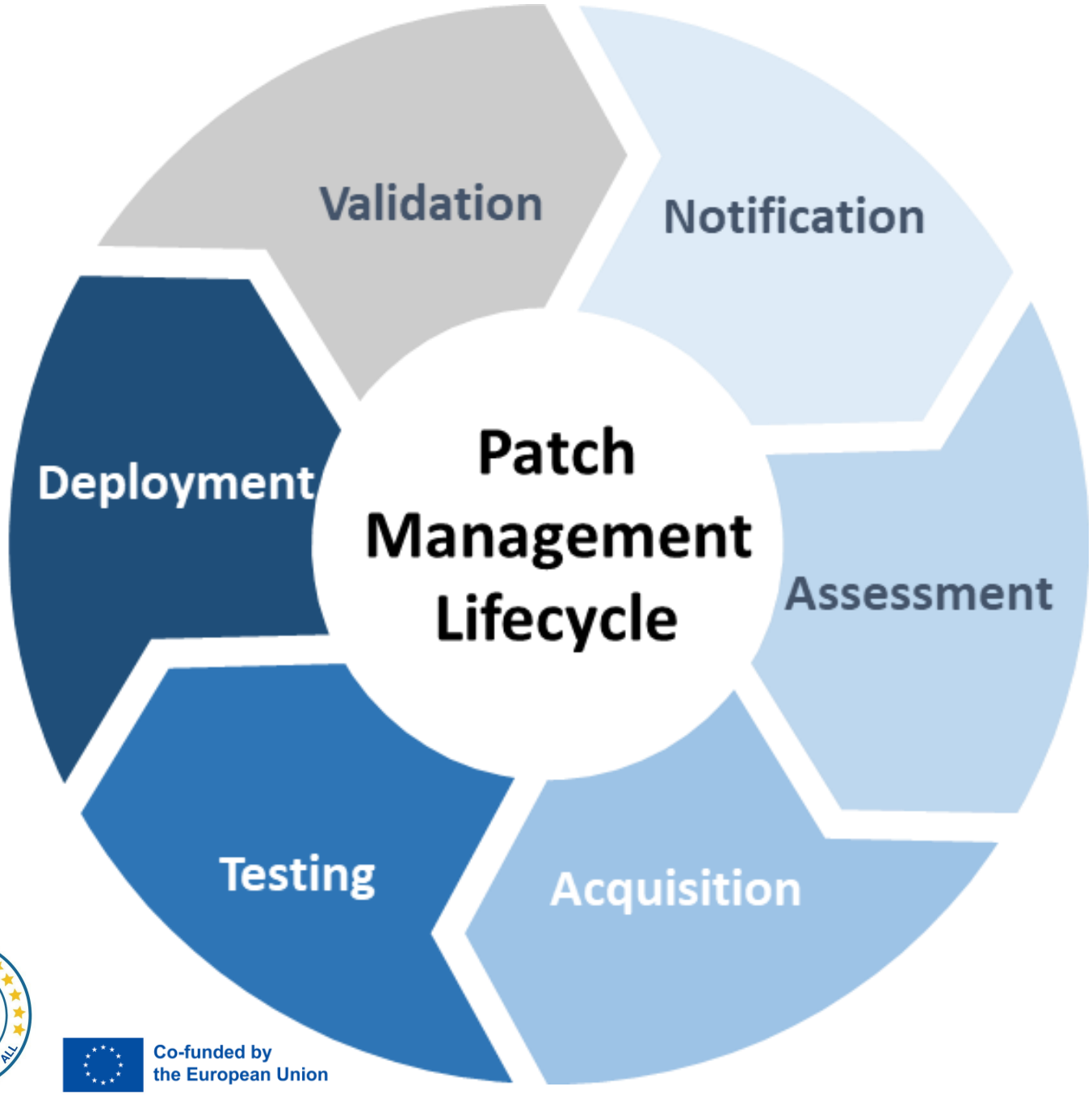
Co-funded by the European Union

Example

if a patch management system finds a connection issue and resolves it, then a developer may refer to the resolution as a patch.

1. **Scan for issues**
2. **Download a patch**
3. **Perform automated patching**
4. **Report the status of the patch**

Co-funded by the European Union



Co-funded by the European Union

The main stages of the patch management process

1. Identifying
2. Acquiring
3. Testing
4. deploying
5. documenting patches

Co-funded by
the European Union

WHY DO WE NEED PATCH MANAGEMENT?

Co-funded by the European Union

5.6 Network Access Control

- A security solution that uses a set of protocols to keep unauthorized users and devices out of a private network
- give restricted access to the devices which are compliant with network security policies
- Handles network management and security
- Works on wired and wireless networks by identifying different devices that are connected to the network

Co-funded by
the European Union

Components of Network Access Control Scheme

- Restricted Access
- Network Boundary Protection

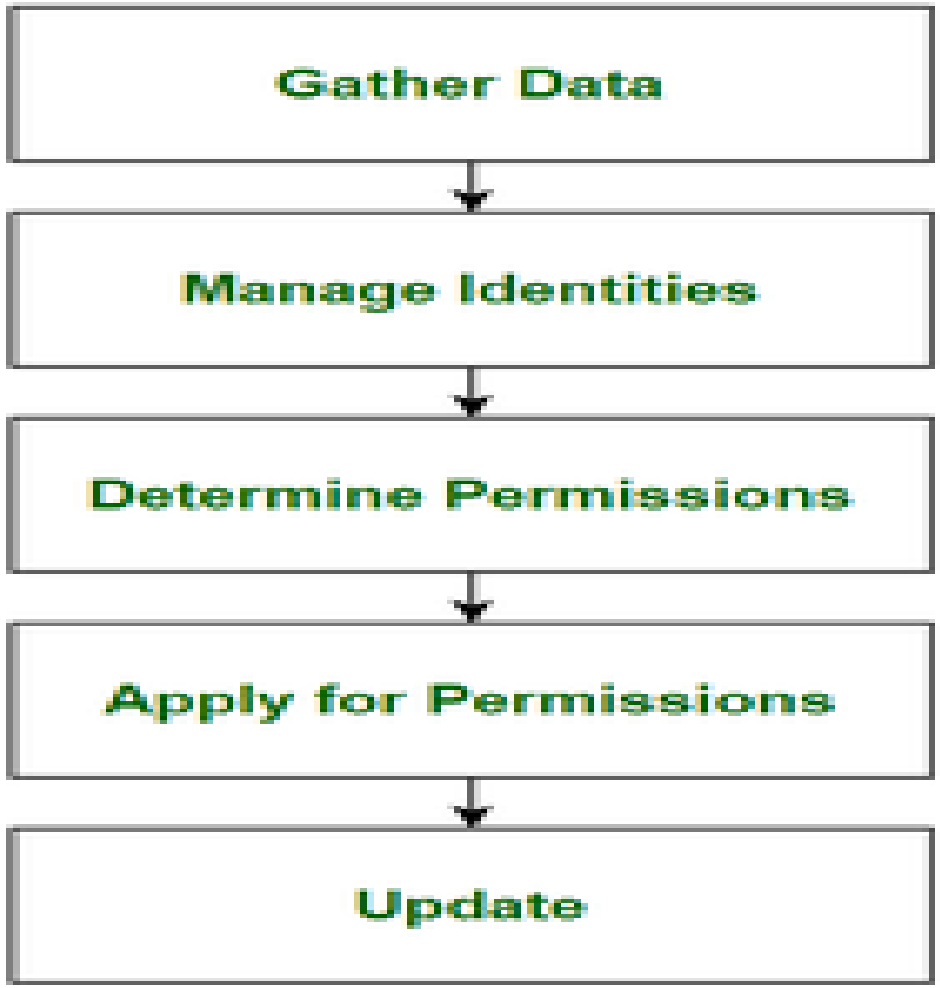
Co-funded by the European Union

Types of Network Control Access

- Preadmission
- Postadmission

Co-funded by
the European Union

Steps to Implement NAC Solutions



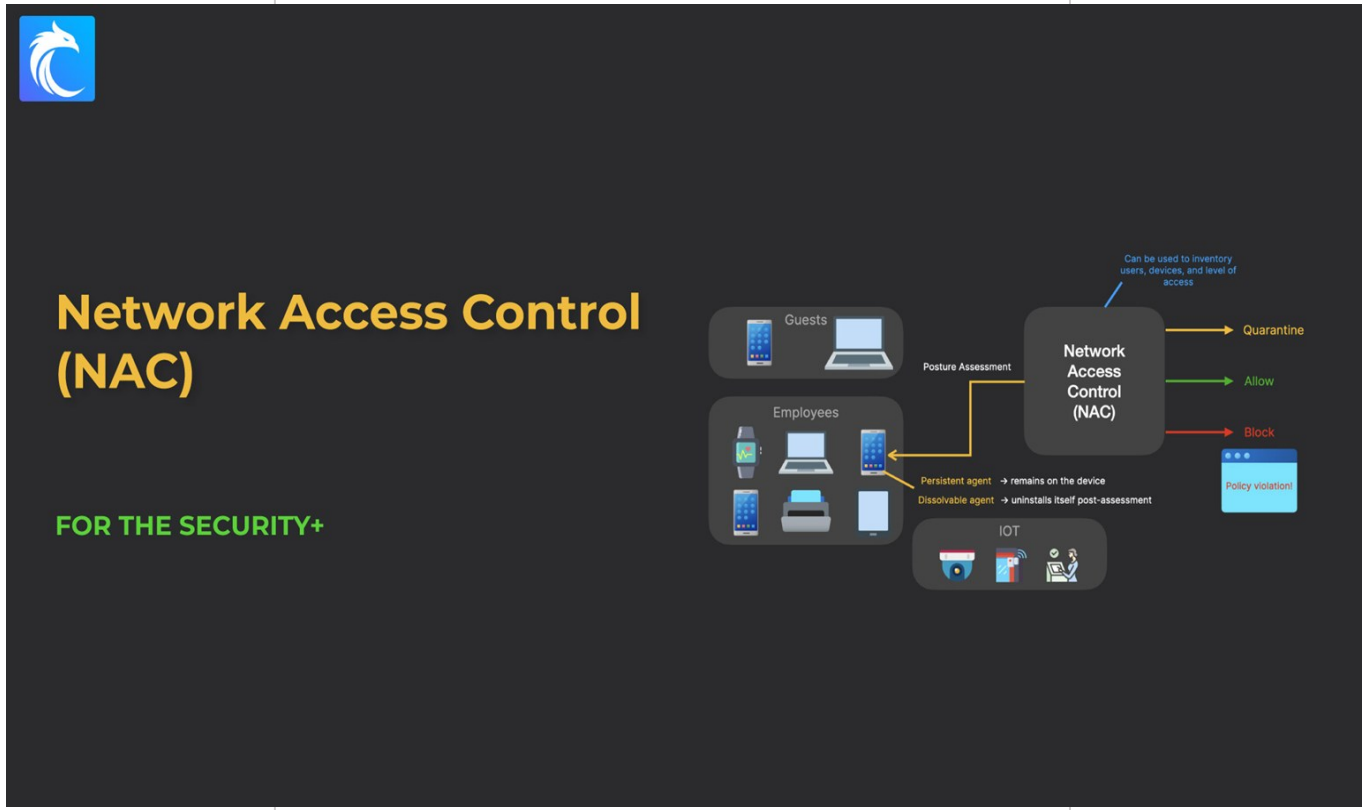
Co-funded by the European Union

Principle Elements of Network Access Control

Access Requestor(AR)

Policy Servers

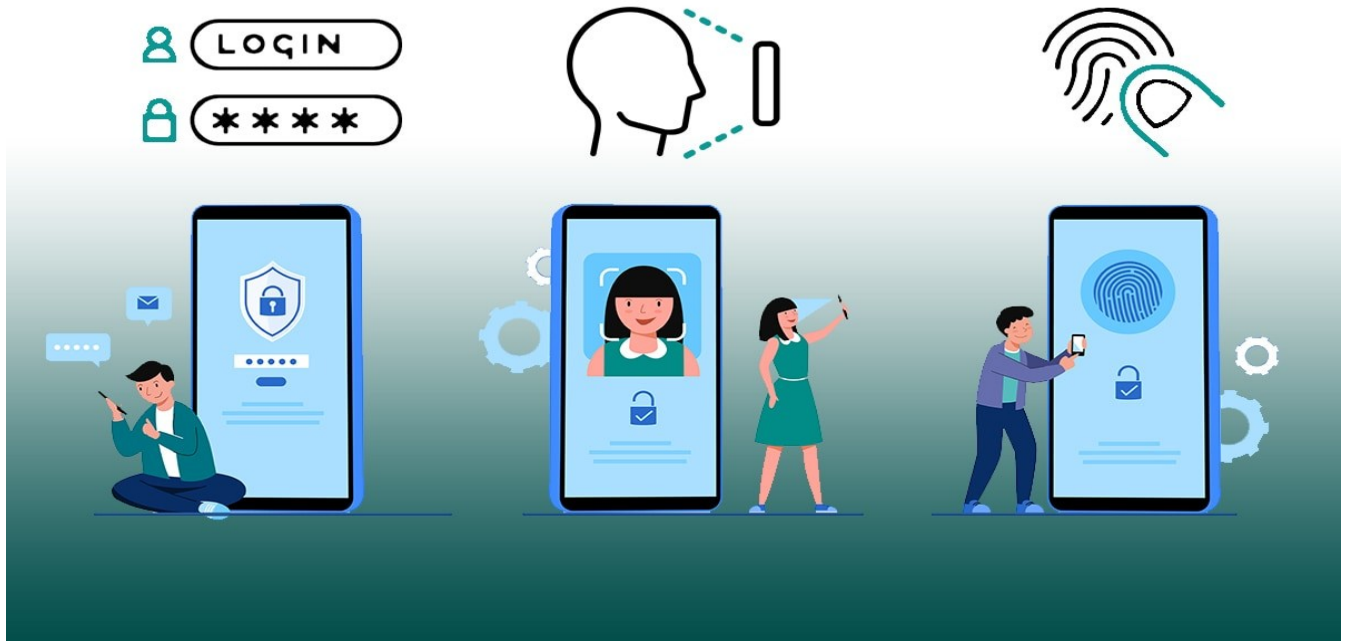
Network Access Servers(NAS)



Co-funded by the European Union

Pros

- Multi-factor authentication
- Additional levels of protection



Co-funded by
the European Union

Cons

- Low visibility in IoT devices and devices
- Does not protect from threats
- Not compatible with existing security controls

Co-funded by
the European Union

5.7 Web Content Filtering

- Websites
- Web Applications
- File Downloads
- Web Protocols
- Streaming Content

Co-funded by
the European Union

What is Web Content Filtering ?

- Analysing web traffic and allowing, blocking, quarantining, or logging that traffic based on rules

- Enterprise cybersecurity, networking, and endpoint security tools like firewalls, secure web gateways, proxies, and endpoint agents

Co-funded by
the European Union

Different Technical methods:

- Blacklisting
- Whitelisting
- URL Filtering
- File Type Filtering
- Bandwidth Limiting
- Data Loss Prevention

Co-funded by
the European Union

Why is Web Content Filtering Important ?

- Security Against WebBased Threats
- Protecting Bandwidth & Productivity
- Regulatory Compliance
- Reducing Legal Liability

Co-funded by
the European Union

Web Filtering Methods and Tools

- Secure Web Gateways (SWG)
- NextGeneration Firewalls (NGFW)
- Web Application Firewalls
- Web Proxies
- DNS Filtering
- Endpoint Web Controls

Co-funded by the European Union

Future...

- Automated Policy Recommendations
- Granular User Controls
- RealTime Threat Intelligence
- Contextual Content Analysis
- SelfHealing Networks

Co-funded by the European Union

5.8 CloudBased Endpoint Protection

Cybersecurity solution designed to secure endpoint devices such as laptops, desktops, servers, and mobile devices through a cloud-based platform

Co-funded by the European Union

5.8 CloudBased Endpoint Protection

- set of practices and technologies that protect enduser devices
- Prevent third party unauthorized entry
- allows IT teams to protect devices more effectively while minimizing their time and effort

Co-funded by
the European Union

Key Features of Cloud-Based Endpoint Protection

- **Centralized Management:** ability to manage all endpoints from a single, unified cloud-based dashboard
- simplifies security administration and allows security teams to monitor and respond to threats in real-time across all devices

- **Real-Time Threat Detection and Response:**monitors endpoints and use artificial intelligence (AI) and machine learning (ML) to detect suspicious activity and automatically respond to potential threats

Co-funded by the European Union

Key Features of Cloud-Based Endpoint Protection

Scalability: highly scalable, making them ideal for organizations of all sizes

As businesses grow, they can easily add more endpoints to the system without needing to upgrade or replace hardware

Advanced Threat Intelligence: integrate threat intelligence feeds from global sources, enabling them to identify new and emerging threats quickly.

Co-funded by the European Union

Key Features of Cloud-Based Endpoint Protection

User Behavior Analytics: helps detect abnormal patterns in user behavior (such as unusual login attempts or file access).

identify insider threats or compromised credentials.

Multi-OS Support: provide protection across multiple operating systems and device types, such as Windows, macOS, Linux, iOS, and Android.

Co-funded by the European Union

Benefits of Cloud-Based Endpoint Protection

- Ease of Deployment
- Cost Efficiency
- Increased Flexibility
- Data Protection and Compliance

Co-funded by the European Union

Why is Endpoint Security important ?

- Data exchanged between the endpoint and the enterprise network
- Remotely install malicious software
- Gain broad access to other critical resources and data assets.
- Endpoint security solutions reduce the risk of such issues

Co-funded by
the European Union

Benefits

- Nearrealtime protection
- Easier management
- Superior patching cadence
- Comprehensive monitoring
- Faster deployment
- Unlimited scaling

Co-funded by
the European Union

Types of Risk does endpoint security minimize ?

Phishing

Ransomware

Internal Security Risk

Co-funded by the European Union

Endpoint Detection and Response (EDR)

Cybersecurity solution designed to continuously monitor, detect, and respond to threats at the endpoint level.

Co-funded by the European Union

Co-funded by the European Union

Endpoint Detection and Response (EDR)

- Detecting and responding to malware threats
- Works by monitoring all incoming and outgoing information
- Need a form of managed detection response

Key Components of EDR

Continuous Monitoring: collects and analyze activity data from endpoints to identify suspicious behavior in real-time

Threat Detection: Using techniques such as behavioral analysis, machine learning, and signature-based detection,identify both known and emerging threats

Co-funded by the European Union

Key Components of EDR

Incident Response: isolating the affected endpoint, terminating malicious processes, or rolling back to a previous, uninfected state

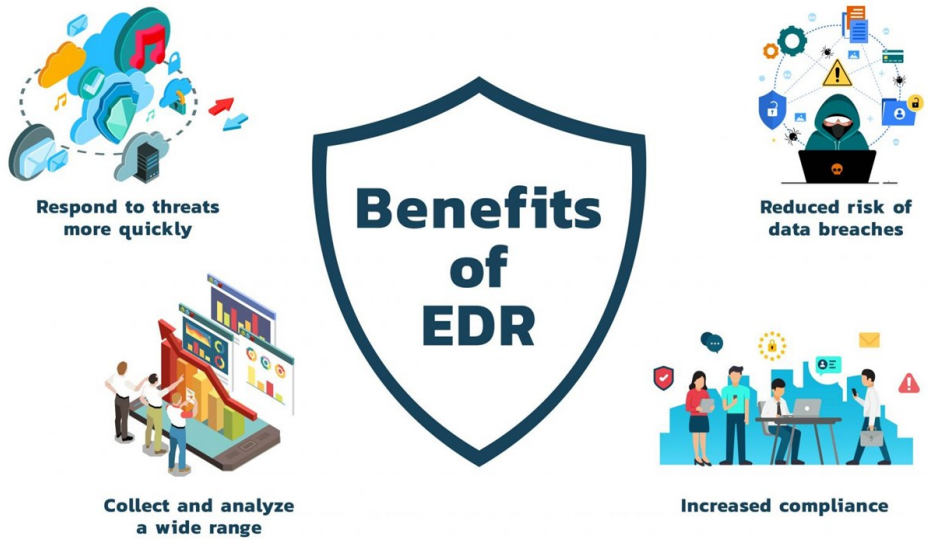
Forensic Analysis: maintain detailed logs of endpoint activity, allowing security teams to investigate past incidents, determine the root cause, and improve future defenses.

Automation: accelerate the response process, minimizing the time between threat detection and remediation

Co-funded by the European Union

Benefits of EDR

- Improved Threat Visibility
- Quick Response to Threats
- Comprehensive Forensics
- Protection Against Advanced Threats



Co-funded by the European Union

Example EDR Solutions

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Carbon Black
- Sophos Intercept

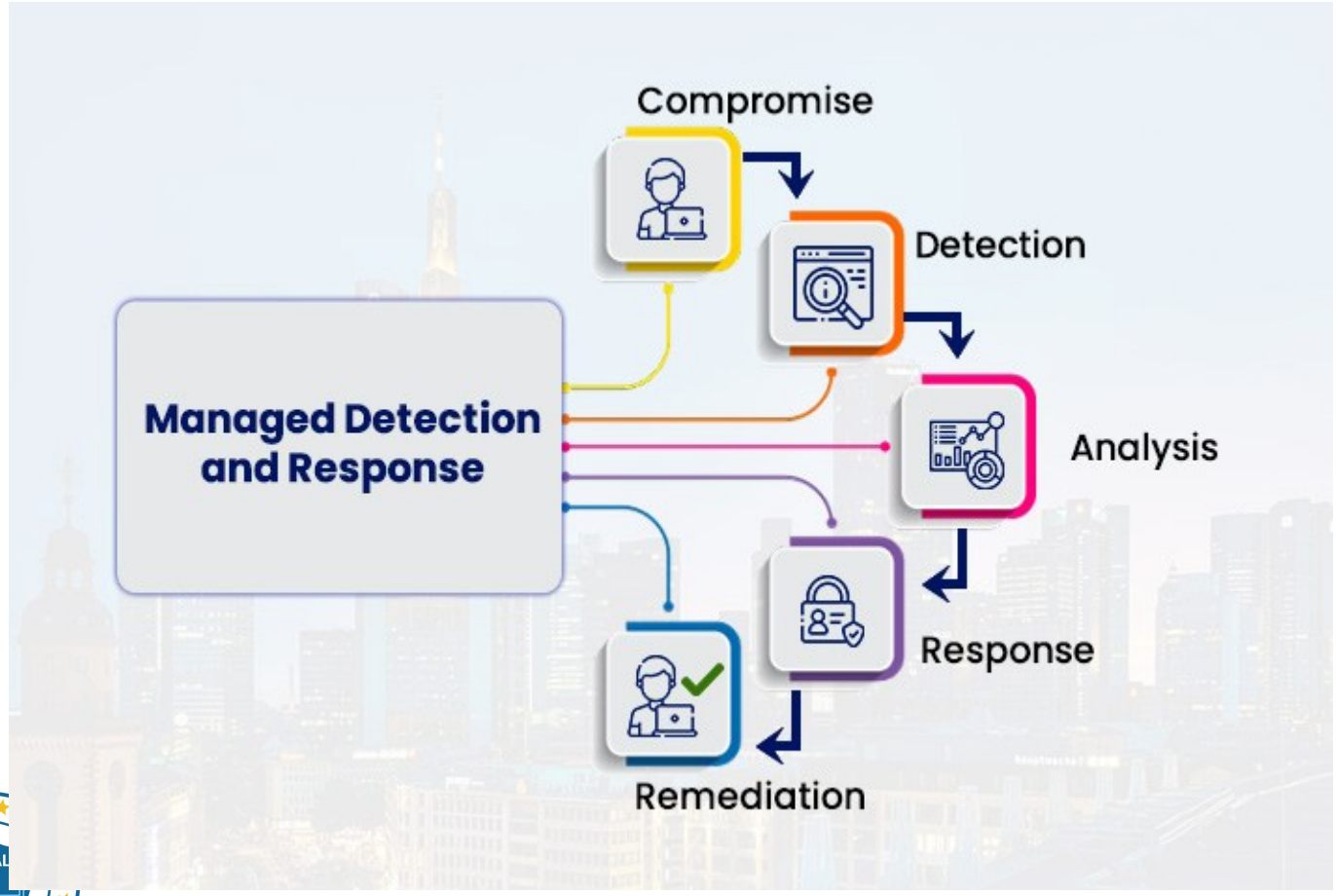
vmware Carbon Black

CROWDSTRIKE

Microsoft Defender for Endpoint

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Managed detection and response (MDR)



Co-funded by the European Union

Managed detection and response (MDR)

Cybersecurity service that provides organizations with 24/7 threat detection, monitoring, and response capabilities, often without the need for in-house security operations.

CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Key Components of MDR

24/7 Threat Monitoring: continuously monitors an organization’s environment, analyzing security events and alerting the team when suspicious activity is detected

Threat Hunting: employ skilled analysts who proactively search for hidden threats within an organization's systems

Incident Response: might involve isolating compromised systems, terminating malicious processes, and guiding the organization through recovery.

Co-funded by
the European Union

Key Components of MDR

Expert Analysis: Access to cybersecurity experts who interpret security data, provide actionable insights, and recommend appropriate responses to complex threats

Advanced Tools and Technology: Combination of tools, including Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and threat intelligence feeds, to provide comprehensive coverage against a wide range of threats

Co-funded by the European Union

Benefits of MDR

24/7 Coverage: With dedicated security experts monitoring your systems around the clock, MDR ensures that no threats go unnoticed

Access to Security Experts: access to seasoned professionals who can enhance the organization's overall security posture.

Faster Detection and Response: advanced tools and human intelligence to detect and respond to threats faster than most in-house teams can manage

Cost-Effective: more cost-effective alternative by outsourcing the expertise and technology needed.

Co-funded by the European Union

Examples of MDR Providers

- Rapid7 MDR
- CrowdStrike Falcon Complete
- Sophos MDR
- Palo Alto Networks MDR
- Arctic Wolf

Co-funded by the European Union

Learning Outcome

- After successful completion of this course, students would be able to:
- Understand the key components of endpoint protection, including antivirus/antimalware, firewalls, patch management, and cloud security, and analyze their roles in securing devices and networks.
- Apply antivirus and antimalware tools to detect, remove, and prevent malicious software on endpoint devices, enhancing protection against cyber threats.
- Utilize firewall protection to control and monitor network traffic and prevent unauthorized access, strengthening endpoint defenses.
- Learn the importance of patch management and demonstrate how to implement it as a critical practice to maintain a secure environment and prevent security breaches.
- Implement cloud security features to secure data access, prevent infiltration, and improve monitoring of user activity, ensuring enhanced endpoint security in cloud-based environments.

Question no 01

What is the primary function of antivirus software?

A. Encrypt data
B. Detect and remove malicious software
C. Monitor network traffic
D. Manage user permissions

Co-funded by the European Union

Question no 02

Which of the following is NOT a type of malware?

A. Virus
B. Trojan horse
C. Firewall
D. Ransomware

Co-funded by
the European Union

Question no 03

Which of the following is NOT typically a feature of endpoint protection software?

A. Firewall protection
B. Data loss prevention
C. Device monitoring
D. Web hosting services

Co-funded by the European Union

Question no 04

What is the primary function of a firewall in a network?

A. To scan for malware
B. To block unauthorized access while permitting legitimate communication
C. To store data securely
D. To encrypt network traffic

Co-funded by the European Union

Question no 05

Which of the following is a potential drawback of application whitelisting?

A. It allows all applications to run by default
B. It requires continuous maintenance to keep the whitelist updated
C. It is less secure than blacklisting
D. It does not work with antivirus software

Co-funded by the European Union

Question no 06

What is the primary purpose of patch management in operating system security?

A. Enhancing user authentication
B. Managing network traffic
C. Improving system performance
D. Closing security vulnerabilities

Co-funded by the European Union

Question no 07

Which term refers to a piece of software designed to fix a security vulnerability or improve the functionality of a program or operating system?

A. Service pack
B. Update
C. Patch
D. Hotfix

Co-funded by the European Union

Question no 08

Which component of an operating system is responsible for managing and applying updates?

A. Update Manager
B. Patch Control
C. Software Updater
D. Windows Update

Co-funded by the European Union

Question no 09

What is the purpose of the Least Privilege Principle in user management and access control?

A. Maximizing user privileges
B. Minimizing user privileges to the minimum necessary for tasks
C. User authentication
D. File encryption

Co-funded by the European Union

Question no 10

What is the primary purpose of patch management in operating system security?

A. Enhancing user authentication
B. Managing network traffic
C. Improving system performance
D. Closing security vulnerabilities

Co-funded by the European Union

Question no 11

Which attribute best describes how early web filters worked ?

A. Web filters use big data comparative analysis
B. Web filters are role based
C. Web filters user heuristics
D. Web filters are rule based

Co-funded by the European Union

Question no 12

How does web filters improve computer security ?

A. They blocked adware, spam, viruses and spyware
B. They tested all URLs is segregated VMs to see what they would do.
C. They block lewd websites
D. They prevented denial of service attacks.

Co-funded by the European Union

Question no 13

The full form of EDR is _____?

A. Endpoint Detection and recovery
B. Early detection and response
C. Endpoint Detection and response
D. Endless Detection and Recovery

Co-funded by
the European Union

Answers

1. **B)** Detect and remove malicious software
2. **C)** Firewall
3. **D)** Web hosting services
4. **B)** To block unauthorized access while permitting legitimate communication
5. **B)** It requires continuous maintenance to keep the whitelist updated
6. **D)** Closing security vulnerabilities
7. **C)** Patch
8. **D)** Windows Update
9. **B)** Minimizing user privileges to the minimum necessary for tasks
10. **D)** Closing security vulnerabilities
11. **D)** Web filters are rule based
12. **A)** They blocked adware, spam, viruses and spyware
13. **C)** Endpoint Detection and response

Co-funded by the European Union

References

- "Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat" S. Chandel, S. Yu, T. Yitian, Z. Zhili and H. Yusheng,
- "Protection of Research Data and Devices from Malware Attacks Using Endpoint Security System in Network" Pratap Singh Solanki1, Ajay Singh, Shaneel Sao, N.D. Atkekar
- Understanding Network Access Control: http://techdata.ca/techsolutions/networking/files/feb2009/Enterasys%20NAC%20Planning%20Guide.pdf
- A complete guide on Endpoint security:https://www.vtechsolution.com/wp-content/uploads/2022/05/ACOMPLETEGUIDEONENDPOINTSECURITY.pdf
- Patch Management: University of PORTSMOUTH: https://userguides.docstore.port.ac.uk/A931230.pdf
- https://www.youtube.com/watch?v=D_q-MzhMENw

Co-funded by the European Union

https://www.cool-waters.co.uk/blog/what-is-endpoint-protection

https://www.aratek.co/news/multi-factor-authentication-how-it-works-and-why-it-matters

https://www.softactivity.com/ideas/insider-threat-statistics/

https://www.goguardian.com/glossary/what-is-content-filtering

https://www.linkedin.com/pulse/boost-your-business-security-microsoft-defender-endpoint-jovan-savage-csf6c/

Co-funded by
the European Union

Reference Book

- "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig, William Pollock publication
- "Cybersecurity for Beginners" by Raef Meeuwisse, Cyber Simplicity Limited publisher, 2nd Edition
- "The Art of Computer Virus Research and Defense" by Peter Szor, Addison-Wesley Professional, 1st edition

Co-funded by the European Union