**Endpoints security technologies**

**Host-based Personal Firewall**

* Personal firewalls protect a single host
* Monitor incoming and outgoing connections
* They have a logging feature that tracks the firewall’s handling of various types of traffic
* Ex of linux host-based firewall variants: Iptables, TCPwrappers

Windows host-based firewall facts: it is enabled by default and we can create: program rules, port rules, predefined rules, custom rules

**Host-based Anti-virus**

* Antivirus software may use heuristics with other methods to detect malware.
* Most antivirus software uses signature-based malware detection.

**Host-based Intrusion Prevention System (HIPS)**

* HIPS is a software package that detects and prevents attacks on the host on which it is installed
* In case of suspicious activity by a hacker or malware, HIPS blocks the action and alerts the user
* Examples of HIPS technologies: signature-based IPS, Anomaly-based IPS, Policy-based IPS, Any combination of the above

**Application Allowed Lists and Blocked Lists**

* Applying a blocked list is a security technique whereby any entity that is found on a blocked list is denied access to resources.
* Blacklisting: allows all traffic that is not explicitly denied
* Whitelist: denies all traffic that is not explicitly permitted

**Host-Based Malware Protection**

* With malware, endpoints must be protected before, during and after attacks
* Cisco AMP for Endpoints is an advanced malware analysis and protection solution

**AMP for endpoint provides:**

* Cloud-based detection of malware through the cisco CSI Cloud
* Rapid detection of known malware by examining the file’s SHA
* Use of cloud resources to test files with unknown dispositions
* Use of machine learning techniques to constantly keep itself up
* Historical perspective so that you can see, over time, the actions that files performed on a system

**Sandboxing**

* is a key part of network security when it operates as an integrated component of a complete solution.
* Sandboxing technology has the ability to emulate an environment, detonate a file without risk of infection, and analyze the file behavior
* Sandboxes detonate unknown files in a safe environment and then record its actions
* Sandbox solution example: cisco threat grid solution

**File Integrity Checking**

* File integrity checking tools determine if files on a system have been modified in any way
* File integrity checking tools are included with most-based IPSs
* File integrity checking tools work by
* Calculating hash values of important files
* Storing the hash values
* Periodically comparing stored hash values to hash values that it calculates later

**AMP**

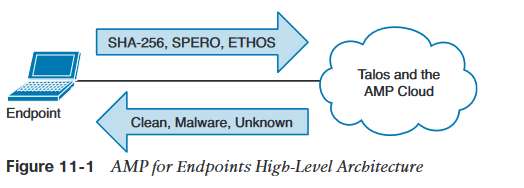
**Advanced malware protection software** is designed to prevent, detect, and help remove threats in an efficient manner from computer systems. Threats can take the form of software viruses and other malware such as ransomware, worms, Trojans, spyware, adware, and fileless malware.

**Endpoint Detection and Response EDR**

* EDR solutions monitor endpoint and network events and record the information in a central database so that you can perform further analysis, detection, investigation, and reporting
* Software (an agent) is installed on the endpoint that allows ongoing monitoring an detection of potential security threats
* EDR capabilities: filtering, threat blocking, help with digital forensics and incident response DFIR (the ability to allow an organization to effectively perform DFIR task
* Endpoint Protection Platform (EPP). An EPP provides not only detection, but also protection (threat blocking). In many cases, people refer to EPP and EDR as the same thing.

**Cisco AMP for Endpoints**

* AMP for Endpoint also provides cloud-based detection of malware
* AMP for cloud provides a historical view of malware activity, segmented into two activity types:
  + **File trajectory** (what endpoints have seen the files), device trajectory and **device trajectory** (action the files performed on given endpoints)
* AMP for Endpoints is the connector that resides on windows, Mac, Linux and android endpoints
* It is remains lightweight, sending a hash to the cloud and allowing the cloud to make decisions and returns the verdicts Clean, Malware, and unknown
* To allows a connector to communicate with cisco cloud server for file and network disposition lookups a firewall must allow the clients to connect with TCP port 443 or TCP port 32137



**Outbreak Control**

* Outbreak Control allows you to create lists that customize AMP for Endpoints to your organization
* Outbreak option: custom detection, application control, network, and endpoint IOC (indicators of compromise)
* Simple custom detection just look for the SHA-256 hash of file
* Advanced custom detection offer more signature types to detection: File body–based signatures, MD5 signatures, MD5, PE section–based signatures  
  An extended signature format (with wildcards, regular expressions, and offsets), Logical signatures, Icon signatures
* Android detection are defined separately from ones used by windows or Mac
* When a malicious app is detected, the user of the mobile device is notified and prompted to uninstall it.

**IP blacklists and whitelists**

* You can use IP whitelist to define IPv4 addresses that should not be blocked
* You use IP blacklists to create DFC (device flow correlation) detections. Traffic that matches entries in the blacklist are flagged or blocked, as the DFC rule dictates.

**Application control**

Like files, applications can be detected, blocked, and whitelisted. As with the other files,

AMP does not look for the name of the application but the SHA-256 hash.

**Exclusion Sets**

An exclusion set is a list of directories, file extensions, or even threat names that you do not want the AMP agent to scan and subsequent

Available exclusion types:

* Threat: This type excludes specific detections by threat name.
* Extension: This type excludes files with a specific extension.
* Wildcard: This type excludes files or paths using wildcards for filenames, extensions,
* or paths.
* Path: This type excludes files in a given path ly not convict as malware.

**AnyConnect AMP Enabler**

You can use the AMP Enabler add-on to AnyConnect to aid in the distribution of the AMP connector to clients who use AnyConnect for remote access VPN, secure network access, posture assessments with Cisco’s Identity Services Engine, and more.

**AMP for Endpoint Engines**

**TETRA**:

* A full client-side antivirus solution. (Do not enable the use of TETRA if there is an existing antivirus product in place).
* When you enable TETRA, another configuration subsection is displayed, allowing you to choose what file scanning options you wish to enable.

**Spero**:

* A machine learning–based technology that proactively identifies threats that were previously unknown.
* It uses active heuristics to gather execution attributes, and because the underlying algorithms come up with generic models, they can identify malicious software based on its general appearance rather than basing identity on specific patterns or signatures.

**Ethos**: A “fuzzy fingerprinting” engine that uses static or passive heuristics

**AMP for Endpoints Reporting**AMP for Endpoints includes a series of reporting dashboards that can be very useful  
to understand what’s happening in your endpoints.

**Cisco Threat Response**

Cisco Threat Response is a “one-pane-of-glass” console that automates integrations across Cisco security products and threat intelligence sources. This is an ongoing effort from Cisco to provide a single console for the management of most of its security products.

Cisco Threat Response integrates with the following Cisco security solutions:

■ Cisco Advanced Malware Protection

■ AMP for Endpoints

■ Cisco Threat Grid

■ Cisco Umbrella

■ Cisco Email Security

■ Cisco Next-Generation Firewalls (NGFW)

■ Next-Generation Intrusion Prevention System (NGIPS)