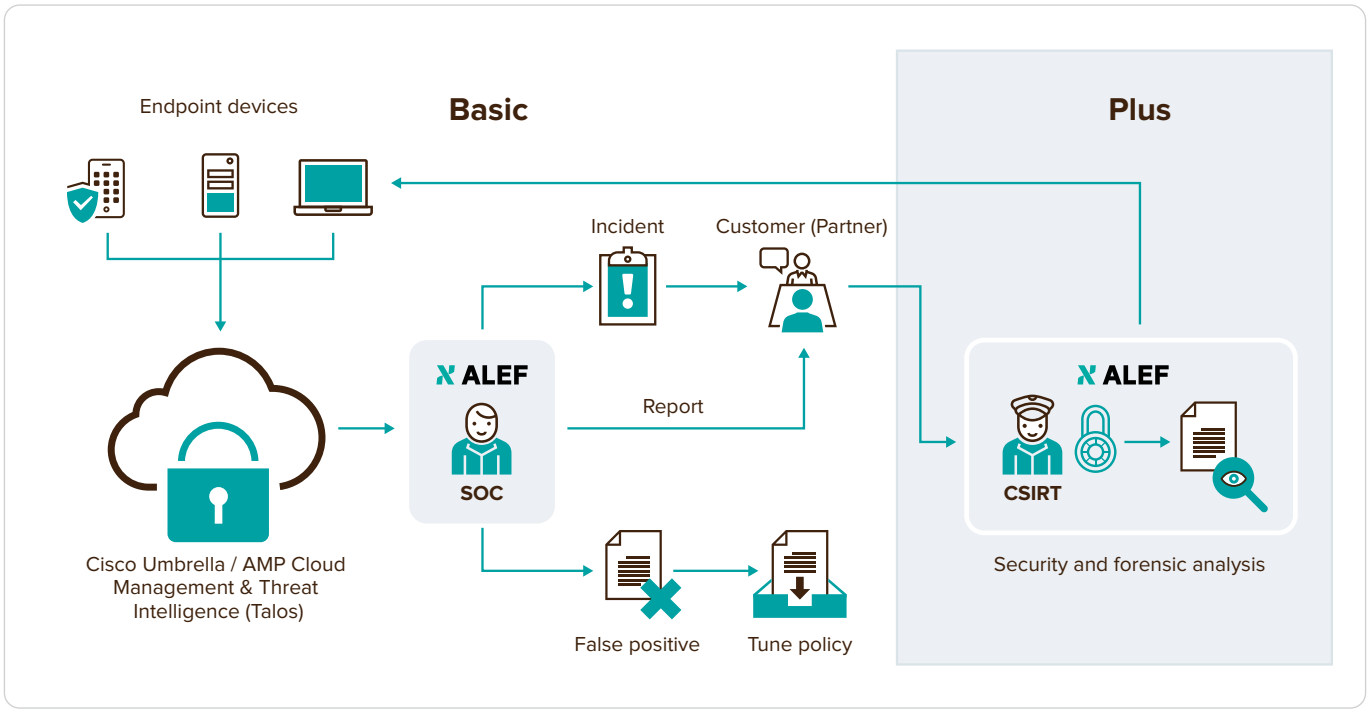
ALEF

ALEF OctoShield

Basic & Plus

The main purpose of the ALEF OctoShield service is to provide a higher security standard for end devices connected to your network or connecting to the Internet from any location. Using our service, you will be protected from a vast majority of malicious software used by the attackers for engaging in cyber-attacks.

We use a combination of cloud products made by Cisco Systems – Advanced Malware Protection (AMP) and Umbrella – offering features going beyond standard antivirus programs. Along with ALEF's security monitoring, we provide customers with very strong and continuous protection from security incidents.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

cisco Partner
Distribution Partner

ALEF

Included in the service

- Continuous protection of end user devices utilising modern cloud products made by Cisco Systems — Antimalware Protection for Endpoints (hereinafter AMP4E) and Umbrella.
- Quick and very effective blocking of any cyber attack on end devices, regardless of whether they are connected to the Internet via your network or outside it.
- In-depth explanation of cyber attacks on endpoint devices and recommendations on how to prevent such attacks in the future.
- Cooperation provided by our experts in implementing preventive measures against further attacks.

WE OFFER SECURITY MONITORING IN TWO VARIANTS – BASIC AND PLUS

ALEF OctoShield Basic

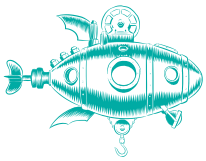
The Basic variant includes:

- Initial activation of AMP4E and Umbrella, where our professional team analyses the current protection status of your network and end devices, proposes the best possible scenario for implementing these two cloud products and fine tunes them to your needs.
- Continuous and automatic protection of end devices from security attacks. The protection works even where a user works outside the company, e.g. home office.
- Continuous monitoring and evaluation of security incidents detected by AMP4E and Umbrella on your end devices by the security team at ALEF Security Operations Center (SOC) in 8×5 mode.
- Basic analysis of detected security incidents on end devices, particularly malware, command, and control callbacks, cryptomining.
- Distribution of regular weekly reports featuring an overview of security events detected on your end devices.
- Forwarding of information on the occurrence, impact, and security risk of a confirmed security incident, including proposals on how to proceed in a specific matter.

ALEF OctoShield Plus

This variant includes the ALEF Incident Response service:

- Resolution of security incidents, including implementation of corrective measures by the ALEF CSIRT security team, which is a registered member of the Trusted Introducer international organisation specialising in cyber security
- In-depth analysis of the malicious code identified in your network by the ALEF CSIRT team
- Security Scan, i.e. regular preventive daily or monthly security scanning of your communication and system infrastructure by a specialised tool; we will provide you with an overview of vulnerabilities of your network and an assessment of their criticality.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TI TRUSTED INTRODUCER

CISCO Partner
Distribution Partner

ALEF

Cisco Umbrella

The Cisco Umbrella technology is irreplaceable as the first line of your network's defence against Internet threats. It uses the basic building blocks of the Internet for this purpose – DNS and IP layer. By securing these two components using the so-called reputation, the Umbrella is able to block requests for malicious or undesirable data sources even before any connection with them is established.

The Umbrella is particularly suitable for end stations moving outside the corporate network, which under normal circumstances provides users with central protection (so-called roaming computers). It operates as a secure Internet gateway using redirection of DNS traffic to Cisco Systems' cloud servers that – thanks to advanced analytics and machine learning – are able to assess whether any queried domain is secure, malicious or suspicious. Moreover, any suspicious domains may be redirected to a cloud proxy for in-depth inspection of whether any transmitted data content (files, scripts, etc.) is in fact secure.

Each day, the Umbrella's global infrastructure evaluates more than 125 billion DNS queries, which allows unique tracing of relationships between domains, IP addresses, networks and malware throughout the Internet as a whole. Similar to how Amazon's systems are able to create customer purchasing patterns and predict their next purchases, the Umbrella learns from online activity of users and creates formulas for automatic uncovering of the attacker's infrastructure. In this manner, it is ready for the next attacks and predictive blocking of all data sources known to it.

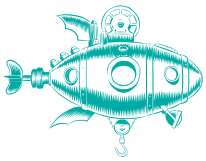
CISCO UMBRELLA'S PROPERTIES

- Reduces malware infections by up to 98%
- Allows filtering up to 60 different domain categories
- Detects any use of cloud applications and displays their use report
- Prevents data leaks from your network or devices
- Protects users both inside and outside the corporate network
- To maintain high level security of end devices, there is no need to have them connected to the corporate network via VPN

Cisco Advanced Malware Protection for Endpoints (AMP4E)

In a rapidly evolving world of malware, the threats get more sophisticated and it is ever more difficult to detect them. The most advanced 1% of these threats could be ultimately able to enter your network and remain undetected. However, AMP4E provides comprehensive protection even against this 1% threat. This security software prevents device intrusion, blocks malware at the entry and continuously monitors and analyses any activity of files and processes so that it is able to quickly detect and remedy any threats that have managed to avoid the first line of defence.

Its biggest advantage over traditional antivirus solutions is its immediate response to threats (no signatures being downloaded) and blocking of all files that form part of a malware campaign, even if by themselves they are not exhibiting any bad activity. AMP4E allows so-called **"Threat Hunting"**, which is the most modern method of looking for signs of cyber threats or ongoing attacks in a large pile of data from end devices.



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8, Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

CISCO Partner
Distribution Partner

ALEF

AMP4E Prevention

File reputation – the AMP Cloud contains a comprehensive database of each file that was ever scanned, including the corresponding good or bad reputation of a file. As a result, any known malware is quickly and easily quarantined at the point of entry to your network without any CPU-intensive scanning.

Antivirus – AMP4E also includes the traditional and constantly updated antivirus signatures for various platforms (Windows, Mac or Linux). The antivirus database is stored locally on each endpoint, meaning it does not rely on a cloud connection when running. This ensures that your end devices are protected both online and offline.

Polymorphic Malware Detection – Malware creators often create multiple variants of the same malware in order to avoid usual detection techniques. AMP4E is able to detect these variants or polymorphic malware using the so-called digital fingerprints (loose fingerprinting). Each digital fingerprint of a suspicious file is then compared with the digital fingerprints of known malware families; where any substantial match is established, the file is immediately blocked.

Machine Learning Analysis – Using algorithms, AMP4E is trained to "learn" to identify any malicious files or activity based on the attributes of known malware. The machine learning features are synchronised in AMP4E with the comprehensive Cisco Talos™ database that provides a better and more accurate analysis model. Working in conjunction, the machine learning in AMP4E is able to assist in detecting previously undetected malware when it first enters your network.

Exploit Prevention – "Fileless attacks" are becoming ever more frequent, with malware attacking the location in memory where the application is loaded. This feature prevents malware from inserting instructions into the memory despite the memory's vulnerability.

Script Protection – AMP4E provides better visibility of execution of any scripts over the end devices, helping protect against any script-based attacks that are frequently used by malware. The script execution control provides an additional protection layer by allowing the Exploit Prevention module to prevent certain DLLs from loading on computers whose applications come with relevant vulnerability.

Behavioral Protection –The improved behavioural analysis of endpoints by AMP4E continuously monitors all activity by users and endpoints and compares it in real time with malware behavioural patterns that are dynamically updated as the malware evolves. Using this method is possible, for example, to detect attacks of "living-off-the-land" type.

AMP4E Detection

Protection from harmful activities – AMP4E continuously monitors all the activity in an endpoint and provides on-the-go detection and blocking of any abnormal behaviour by a program running on the end device. For instance, when any endpoint behaviour indicates ransomware, the detected processes are terminated, preventing the encryption of an endpoint and stopping the attack.

Cloud Indicators of Compromise – Talos is a leading cyber threat analysis organisation that constantly analyses all malware to discover new types of threats and create behavioural and forensic profiles for any emerging threats, otherwise known as Indicators of Compromise (IoC). The obtained forensic data, such as file locations, names of processes, or modifications of registry key values, may assist administrators in finding systems that have already been compromised.

Host IoC – Administrators can write their own IoCs for use in responding to incidents to scan for any Indicators of Compromise on all end stations on which AMP4E is installed.

The IoCs themselves are written in the open standard format (OpenIOC), which makes it easier to utilise data coming from any existing information channels.

AMP4E Response

Given the ever increasing number and growing variety of advanced threats designed to evade precautionary measures, any attempt to breach the network's security should be considered an incident.

This setup should deploy a powerful set of tools to help you easily identify any infected end devices and understand the extent of an attack. In addition to more prevention and detection features, AMP offers granular visibility of end devices and tools for a fast and effective response to security incidents.

Endpoint Forensics – Powerful tools, such as trajectory of files and trajectories of devices, which utilise AMP4E's continuous analysis capabilities to display the full scope of an attack. AMP4E identifies all affected applications, processes, and systems to determine the primary infection, as well as the attack method and the point of infection. These features will help you quickly understand the extent of the problem by identifying all the paths (vectors) used by the attackers to gain access to the system.

Dynamic Analysis – AMP4E includes an integrated and highly secure isolated space environment that leverages Cisco Threat Grid technology to analyse the behaviour of suspicious files. The file analysis generates detailed information about the files, including the severity of their behaviour, original file name, screenshots while executing malware code and the capture of sample packets. Armed with this information, you will better understand what is necessary for suppressing the outbreak and blocking any future attacks.

Command Line Visibility – the visibility of command line's arguments helps determine whether any legitimate applications (including Windows system tools) are in fact being misused for malicious purposes.

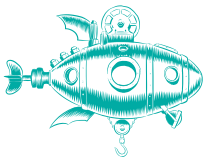
AMP4E is able to identify difficult-to--detect behavioural patterns, such as:

- use of vssadmin to remove shadow copies
- safe boot deactivation
- use of PowerShell,
- execution of priviledge escalation
- modifications of access control lists
- System enumeration.

Retrospective Security – AMP4E uses patented technology that automatically detects advanced threats that have entered your environment. With continuous monitoring, AMP for Endpoints correlates new threat information with your past history and automatically quarantines files as they begin to behave maliciously. This automated response to latest threats provides faster detection time and significantly reduces the spread of malware.

Advanced Search – The Advanced Search simplifies threat investigation and detection by providing more than one hundred pre-prepared queries, which allows you to quickly execute complex queries on any (or all) end devices. This enables you to get a deeper insight into what happened to a particular end device and when, thanks to the snapshot of its current state. Whether you are conducting investigations as part of responses to incidents or detecting any threats, the advanced search will quickly provide you with answers you need to know about your end devices.

Should you have any questions, do not hesitate to contact us: cz-sales@alef.com



Trust the Strong

ALEF Distribution CZ, s.r.o. | Pernerova 691/42, 186 00 Praha 8,
Česká republika | Phone: +420 225 090 240
cz-sales@alef.com | www.alef.com

ACCREDITED BY TRUSTED INTRODUCER

CISCO Partner
Distribution Partner