ALEF

Trust the Strong

Welcome to the world of Cisco technologies, where security is our top priority.

This document provides an overview of the wide range of security solutions ALEF offers in partnership with Cisco, designed to protect your digital environment against evolving threats while supporting smooth and efficient workflows. From advanced internet traffic protection to sophisticated email defense, including whole concept solutions, ALEF is ready to ensure peace and security for your organization.

Secure Access

Cisco Secure Access, a key component of the SASE concept, represents an innovative cloud security solution that ensures smooth and secure user access to any application, port, or protocol.

This solution integrates several key modules - Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Firewall as a Service (FWaaS) - and complements them with other advanced features such as multi-dimensional data loss prevention (DLP), DNS security, browser isolation (Remote Browser Isolation - RBI), and sandboxing, all under the auspices of Talos threat intelligence. Cisco Secure Access provides organizations with the ability to secure their internet traffic with unprecedented flexibility and scope. From visibility and control of non-web traffic with FWaaS, through providing application-based access with ZTNA, to logging and inspecting web traffic for greater transparency and protection through SWG, Secure Access offers comprehensive protection in a multi-layered approach. In addition to detecting and managing cloud applications through CASB, Cisco Secure Access also strengthens the security architecture with modern solutions such as RBI and sandboxing. This combination of features ensures that any network connection is made securely and efficiently while respecting the ever-evolving cyber space.

Although Secure Access may seem complex, it is instead oriented towards simplicity, both for administrators and users. This means the ability to set all security from one place, regardless of the type of connection and destination the user accesses. For users, this is even more tangible, as the user does not have to worry about how and whether they need to connect somewhere, they just select their destination and work.

Umbrella

Cisco Umbrella is long known as an excellent solution for protecting internet communication through DNS filtering. However, today Umbrella represents much more than just DNS protection.

The platform offers a wide range of integrated tools in a user-friendly cloud dashboard, allowing users to comfortably manage their security policies and tools. From this centralized location, policies can be efficiently managed not only for basic DNS protection but also for advanced Web proxy and professional firewall. Cisco Umbrella thus provides comprehensive protection for your headquarters, branches, and individual users outside the secured network, protecting them against internet threats from anywhere in the world.
In addition, Umbrella offers features such as DLP (Data Loss Prevention) and CASB (Cloud Access Security Broker), further enhancing your company's protection. DLP prevents the insertion or sending of sensitive data through text fields or communication with artificial intelligence. CASB then checks whether users are accessing cloud resources correctly and whether unauthorized data storage is occurring. Cisco Umbrella offers the opportunity to try all its features free of charge for 30 days, allowing users to gain practical experience with this advanced security platform.

DUO

Cisco DUO is a recognized cloud service that emphasizes increasing security through Multi-Factor Authentication (MFA).

Offered for free for accounts with up to 10 licenses, DUO focuses on securing through MFA, a fundamental but key layer of defense for any organization. Additionally, the DUO service supports a wide range of applications for integration, allowing broad compatibility with various systems and platforms.Besides MFA, Cisco DUO offers a series of other advanced security features. These include Health Check, which provides an overview of device health before allowing access, and Risk-Based Authentication, which allows for dynamically assessing risk based on user behavior and context. Adaptive access policies and support for the Zero Trust model are other strong aspects of Cisco DUO, increasing its effectiveness in the dynamic environment of modern IT networks.

It is important to note that every access attempt through DUO is carefully verified, authorized, and logged. This feature provides important insight and audit capabilities that are essential for effective management of security policies. Cisco DUO represents a solution that is easy to integrate and user-friendly, offering robust protection without compromising the smoothness and efficiency of work processes. Its use is key for organizations seeking a comprehensive, yet easily manageable security solution to protect their data and systems.

ISE

Cisco ISE (Identity Services Engine) is often called the heart of a secure network. This product is a key element for effective access management to your network.

ISE, you get a complete overview of all devices trying to connect to your network - whether through cable, WiFi, from inside the company, or via remote access. Cisco ISE effectively registers all connection attempts and, based on carefully set static or dynamic rules, allows or restricts access. These rules can be specifically tailored for specific media, people, or situations. With properly segmented networks and ISE functions, you can ensure that the right people have access to the right resources, while unauthorized access is effectively blocked.Cisco ISE also offers advanced features for detecting detailed information about devices, such as the status of the operating system or the version of installed applications. Based on this information, the system can dynamically adjust access rules.

Another advantage of ISE is its ability to work closely with other Cisco products, including firewall solutions, identity stores, or Cisco DNA Center. This integration increases the efficiency and security of the entire network. Cisco ISE is suitable not only for small LAN networks but is designed to be implemented into large multi-cloud environments, providing a high degree of flexibility and scalability for various business needs.

Secure Firewall

Cisco Secure Firewall represents a crucial element in network security, providing broad protection against various cyber threats. Its core functions include stateful inspection (a technique for monitoring the state of active network connections) and support for VPNs, ensuring secure connections between different locations and protecting data during transmission.

A major component of Cisco Secure Firewall is Application Visibility and Control (AVC), which offers users thorough insight and control over application traffic. This feature allows for effective monitoring and regulating access to applications while maintaining network security. Encrypted Visibility Engine (EVE), a unique feature, enables insights into encrypted traffic and detection of threats hidden in encrypted communication without decryption.

The firewall also includes an Intrusion Prevention System (IPS) based on SNORT3, whose dynamic database is updated every 5 minutes. This system actively monitors network traffic and identifies potential security threats and attacks, enhancing an organization's ability to face threats.

Other separate features include URL Filtering and Malware Defense (AMP). URL Filtering gives organizations greater control over web traffic by allowing them to filter and regulate access to websites based on their content and categories. Malware Defense (AMP) provides comprehensive protection against malware, including advanced detection and prevention.Cisco Secure Firewall is an ideal solution for organizations seeking comprehensive protection against a wide range of internet threats, with the ability to customize and expand protection according to specific needs and requirements.

Secure Endpoint

Cisco Secure Endpoint, formerly known as AMP for Endpoints, is a key tool in the arsenal of cybersecurity, providing powerful threat protection and response for a wide range of devices, including Windows, Mac, Linux, Android, and iOS.

This solution is designed to provide comprehensive endpoint protection against a wide range of cyber threats.

Key features of Cisco Secure Endpoint include the ability to continuously detect malware both in real-time and retrospectively. The system thoroughly records file activity, allowing for tracking the spread and extent of malware and identifying the impact and extent of infection.

Integration with global threat information from Talos enhances Cisco Secure Endpoint's ability to face threats. This solution provides organizations with extended insight, context, and control for effective detection and response to Command & Control attacks, protection against ransomware, and other sophisticated threats.

Cisco Secure Endpoint is equipped with advanced features such as Orbital for proactive threat hunting and vulnerability management, enabling organizations to quickly identify and address potential security weaknesses in their systems.

These features are key to modern cyber defense and help keep organizations one step ahead of potential attackers.

The easy deployability and management of Cisco Secure Endpoint, along with flexible subscription and an intuitive web interface, make it an ideal solution for organizations of all sizes seeking strong protection for their endpoints in today's dynamic cyber environment.

Secure Web Gateway

Cisco Secure Web Gateway, also known as Web Security Appliance (WSA), represents an advanced solution for securing web traffic.

With integration to global threat information from the Cisco Talos team, Secure Web Gateway provides effective protection against zero-day and advanced threats. This solution combines multi-layered malware protection and real-time traffic analysis with advanced web reputation filters. The breadth of settings allows tuning Secure Web Gateway specifically for your environment, achieving strong security while minimizing restrictions for your users.

Centralized policy management and reporting, along with an extensive overview of web application usage, increase visibility and control over internet traffic. Cisco Secure Web Gateway is integrated with the Cisco XDR platform, accelerating incident response and enhancing collaboration between teams.

Designed for easy configuration and management, Cisco Secure Web Gateway includes data loss prevention features and improves user experience, such as efficient authentication and header rewriting.

This solution represents the ideal combination of advanced security protection and user-friendliness for organizations of all sizes.

Secure Email

Cisco Secure Email, formerly known as Email Security Appliance (ESA), has a long and successful history in protecting email communication.

This solution provides comprehensive protection against a wide range of email threats, including spam, phishing, ransomware, and Business Email Compromise (BEC).

Cisco Secure Email effectively detects and blocks threats using advanced threat intelligence and machine learning, fights sophisticated malware, and reduces its impact. With features such as real-time URL analysis, advanced email identity authentication, and Data Loss Prevention (DLP) with encryption capabilities, Cisco Secure Email protects organizations against phishing attacks and BEC threats.

In addition to basic functions, Cisco Secure Email can be expanded with the Email Threat Defense addon, which enhances Office 365 security by providing an additional layer of protection even for internal email communication. Cisco Secure Email is characterized by a high degree of variability and flexibility, allowing organizations to customize the solution according to their specific needs and requirements. With this adaptability, it provides robust and efficient protection against the constantly evolving email threats.

XDR

Cisco XDR transforms the approach to threat detection and response in the cyber world.

This solution uses Cisco's proven technology to block advanced email threats such as ransomware, business email compromise (BEC), phishing, spoofing, and spam, from both external and internal (East/West) email transmissions. With this solution, a new chapter in security data integration opens, where the use of artificial intelligence and machine learning not only provides an expanded overview of current threats but also accelerates and makes the processes of their detection and neutralization more efficient. Cisco XDR is developed as an independent product and is not limited to extended EDR functions.

It offers a unique combination of visibility across various security layers and integration with a wide range of tools, allowing flexible customization of protection for each organization. This makes it possible to effectively identify and respond to threats, thereby strengthening the defensive capabilities of security teams. The uniqueness of integration in XDR is that it offers integration of third-party tools. With Cisco XDR, you are not limited to Cisco solutions, but you can use information from all your tools.
A specific benefit of XDR is the ability to prioritize threats and accelerate responses. This functionality is invaluable for SOC analysts, who can focus on the most serious threats and streamline investigation processes. Cisco XDR represents a key component of modern security strategies that require a dynamic and proactive approach to protection against the constantly evolving threats in the digital world.

Secure Client

Cisco Secure Client, formerly known as AnyConnect, is a modular client for end devices. It offers the flexibility of deploying necessary modules according to specific requirements and functions. Various security technologies from Cisco use Cisco Secure Client for information collection and device control.

One of the main modules is AnyConnect, which provides VPN functions and enables secure endpoint connections to the network. Another module, Secure Endpoint (EDR), ensures device control and provides real-time threat protection. This module plays a key role in detecting and responding to security incidents.

In addition, the ISE (Identity Services Engine) module can be integrated into Cisco Secure Client, ensuring device posture verification before the device is authenticated for access to the secure network. This module helps ensure that connected devices meet the security standards and policies of the organization.

Secure Client is a unified client across Cisco security products and offers high variability in support of operating systems such as Windows, Linux, macOS, iOS, Android.

Secure Email Threat Defense

Cisco Secure Email Threat Defense, formerly known as Secure Email Cloud Mailbox, represents advanced email protection that addresses potential gaps in Microsoft 365 security.

This solution uses Cisco's proven technology to block advanced email threats such as ransomware, business email compromise (BEC), phishing, spoofing, and spam, from both external and internal (East/West) email transmissions.
Key benefits of Cisco Secure Email Threat Defense include enhancing Microsoft 365 security within minutes without the need to change email flow. This solution provides a complete overview of incoming, outgoing, and internal messages, which is key to effective protection against sophisticated email threats.
Cisco Secure Email Threat Defense strengthens email security by integrating with existing Cisco security technologies, providing robust protection against a wide range of threats. With this solution, organizations gain a powerful tool to combat the latest and most sophisticated threats targeting email communication.

ALEF Group
www.alef.com

ALEF is a reliable supplier of information technologies since 1994. We became one of the largest and strongest value-added distributors in the Eastern Europe – with offices in Czech Republic, Slovakia, Hungary, Slovenia, Croatia, Serbia, Romania and Greece.

The ALEF Group currently employs almost 500 people and has more than 20 professionally equipped training rooms in 7 CEE countries with more than 50 expert trainers and nearly 300 courses offered.

Thank you for your interest in Cisco security solutions. We are here to help with any questions or needs about these products. You can try our some solutions with trial licenses to see their benefits for your organization directly. For more details, webinars, or to set up a meeting to discuss your specific needs, feel free to reach out to our sales team.

Find the closest ALEF office in your region:

https://www.alef.com/en/contact.c-24.html

30th ALEFERSARY

Cisco Distributor