Cisco Security Step-Up

The bridge to possible

Contents

Targeted cyber attacks persist and IT teams are overwhelmed

Phishing is one of the most common and highly successful attack techniques used by cybercriminals. It typically uses social engineering tactics to send targeted emails containing malicious file attachments or links which direct unsuspecting users to phishing domains. These phishing domains can be fake login pages to compromise credentials or could host malware or command and control (C2 or C&C) tools that are downloaded on to the user's device.

To make matters worse, organizations are challenged by budget cuts, lack of cybersecurity expertise and lengthy deployment schedules. When it comes to managing security, 56% of large companies handle 1,000+ security alerts each day while 70% of security professionals have seen alerts double in the past 5 years. (Source: 2020 State of SecOps and Automation Report)

Consolidated security approach stops threats from reaching users

To help protect organizations who need to keep their users safe from threats wherever they access the Internet and need to protect their resources against unauthorized access, Cisco Security Step-Up brings together security solutions that deploy quickly, provide effective protection, are easy to manage, and reduce total cost of ownership.

Overview

Cisco Security Step-Up provides cloud-delivered solutions that significantly reduce incidents and the risk of breaches by combining leading internet threat protection, email security and trusted access capabilities.

Here is what is included:

Internet threat protection:

Inspect web traffic to block internet-borne threats.

- Protects against phishing, ransomware, malicious browser ads, unsolicited cryptomining, information stealing malware and other threats
- Helps unlock internet-wide visibility across all locations, devices, and users – on and off the corporate network
- Offers deep visibility into cloud apps used across the business with risk scoring, blocking and activity controls
- Blocks the loss of sensitive data leaving the organization, unintentionally or maliciously
- Blocks threats before they reach your network

Email security

Protect against threats and attacks carried via email.

- Identifies the malicious techniques used in attacks targeting your organization
- Provides unparalleled context for specific business risks
- Offers searchable threat telemetry
- Categorizes threats to understand which parts of your organization are most vulnerable to attack

Trusted access

Secure access to corporate applications and resources, cloud or on-premises.

- Protects against credential theft by preventing unauthorized access and use of stolen and compromised credentials
- Empowers users with self-service capabilities such as resetting active directory passwords, managing their authentication devices, or updating and remediating those devices so they can be granted access
- Enforces access control across managed and unmanaged devices, including Bring Your Own Device (BYOD)

Feature Details

For organizations who need to protect their users and secure access to resources everywhere, Cisco Security Step-Up provides powerful protection across multiple lines of defense to efficiently keep businesses secure.

Delivered from the cloud for simple and fast deployment, it protects against phishing, ransomware, stolen credentials, malware and other threats, regardless of the user location or the type of infrastructure, whether cloud-based, on-premises, or hybrid.

These three products are included in Cisco Security Step-Up:

Cisco Umbrella Secure Internet Gateway (SIG)

Cisco Secure Email Threat Defense

Cisco Duo

Cisco Umbrella Secure Internet Gateway – inspect web traffic to block internet-borne threats

Secure Web Gateway (SWG) full proxy	Cloud-based full proxy for deeper, granular control of web traffic, including encrypted traffic.
DNS-layer security	This is the first line of defense against threats because DNS resolution is the initial step in internet access. DNS requests precede the IP connection, enabling DNS resolvers to log requested domains over any port or protocol.
Cloud-delivered firewall with Intrusion Prevention System (IPS)	Layers 3, 4, and 7 application visibility and control; Provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. IPS examines network traffic flows and prevents vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection.
Data Loss Prevention (DLP)	Umbrella's cloud-based data loss prevention (DLP) functionality analyzes sensitive data both inline in real time via SWG proxy and out-of-band via restful API to provide visibility and control over that sensitive data leaving your organization.
Remote Browser Isolation (RBI)	Available as an optional add-on, RBI isolates web traffic from the user device and the threat.

Cisco Secure Email Threat Defense – check and analyze emails to stop email delivered threats

Augmentation of native Microsoft 365 security	Adds an additional layer of security to native Microsoft 365 email security by using industry-leading threat intelligence from Cisco Talos, Cisco Secure Endpoint and Secure Malware Analytics–including vast cross-vector threat intelligence from web, network, and endpoint-based sources.
Powerful and searchable threat telemetry capabilities	Quickly evaluates threat data to identify specific threat targets, understand threat techniques and business risk, speed tactical response, and guide strategic planning.
Complete visibility across your messaging environment	Gain insight into all messages in the mailbox in all directions – inbound, outbound, or internal. It allows administrators to search messages across all mailboxes.
Detection and blocking of more threats more quickly	Superior threat intelligence from Cisco Talos provides broader and deeper threat data that informs better and faster decision making. It has an API-enabled architecture for faster response times, complete email visibility, including internal emails, a conversation view for better contextual information, and tools for automatic or manual remediation of threats lurking in Microsoft 365 mailboxes.
More threat context	Integrating with, and sharing key telemetry with, other architecture across the Cisco Secure ecosystem provides actionable insight.
Greater operational efficiency	Easy to deploy and use interface saves time and reduces burden on the team for configuration, investigation, and remediation.
Identification of business risk	Sophisticated Artificial Intelligence, machine learning and natural language processing provide visibility into advanced threat techniques like business email compromise, account takeovers and phishing to track anomalies and understand intent.
More robust threat data	Third-party integration partners add robust features and functionality to further enhance security posture.

Cisco Duo – implement strong authentication to prevent unauthorized access

Multi-Factor Authentication (MFA)	Duo prevents breaches by stopping the use of stolen credentials (username and password). In addition, the Duo Verified Push capability protects against attacks such as push phishing that attempt to bypass MFA.
Passwordless Authentication	Duo simultaneously increases user productivity and security with the ability to securely login without a password. Duo's seamless implementation of passwordless enables organizations to easily transition to passwordless.
Single Sign-On (SSO)	Provides users with an easy and consistent login experience for every application, cloud or on-premises; cloud-based and hosted by Duo, SSO is easy to set up and manage and it is a key step to your passwordless journey.
Device Trust	Duo Device Trust delivers two key capabilities, the Duo Device Health Application and Trusted Endpoints. Together, they provide organizations with the visibility needed to verify the trustworthiness of laptops and desktops and enable administrators to block access attempts from devices that fail health and security posture checks.
Adaptive Access Policies	Allows organizations to easily implement the Zero Trust principle of "least privilege" by ensuring that only the right users, with the right devices, are accessing the right applications.
Risk-Based Authentication	Boosts end-user productivity while ensuring security by adjusting authentication requirements in real time based on the risk level posed by the user and their device.
Duo Trust Monitor	Offers unique visibility into suspicious login attempts taking place outside the control of an organization, allowing otherwise undetectable attacks to be detected as early as possible.
Duo Network Gateway	Enables seamless and secure remote access to on premises and hybrid cloud hosted private applications without requiring VPN; this allows organizations to provide frictionless access experience to users without exposing the applications to the public internet.

Summary

Only Cisco offers the breadth of security solutions to protect all critical attack vectors – web traffic, email and user credentials. Organizations can consolidate their security solutions with Cisco and get the benefits of lower TCO and higher security efficacy.

To register for a free trial of any of these products, go to the following links:
Cisco Secure Umbrella (includes Secure Internet Gateway)
Cisco Secure Email Threat Defense
Cisco Duo

To learn more about Cisco Security Step-Up, sign up here.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

1084512676 05/23