Cisco Umbrella

timico

Five reasons for the rise of the secure internet gateway

Security in a mobile, cloud-enabled world

The way we work has changed

Branch/field offices

70%

connect directly to the internet[1]

Workforce

49%

are mobile workers[2]

Applications

70%

increase in SaaS app use[3]

Security must also change

Built to solve the security challenges of today's mobile, cloud-enabled enterprise, a new category of products is emerging — the secure internet gateway.

Traditional Security vs. Secure Internet Gateway

82% of mobile workers admit that they do not always use VPN when working[4]

Enforcement only on your network

Perimeter security provides visibility and control for employee activity only when on your corporate network.

Enforcement everywhere

A secure internet gateway protects all devices on your network and roaming users.

15% of malware command and control (C2) callbacks use ports other than 80/443 to exfiltrate data[5]

Protection against threats over web

Web gateways only protect employees from threats over web ports 80/443.

Protection over all ports and protocols

A secure internet gateway provides comprehensive protection over all ports and protocols.

60% of the time attackers penetrate and compromise an organisation within minutes, while detection takes days or more[6]

Threat intel from only static reputation scores

Traditional security neutralises threats only after detection. Appliance processing power limits hardware-based tools.

Threat intel from live internet requests

A secure internet gateway uses real-time threat intelligence from global internet activity to uncover attacks before launch. And, because it's cloud-delivered, it's not limited by appliance CPU.

Some companies use up to 50 different security vendors[7] and generate almost 17,000 alerts per week[8]

Limited integration

You likely have many different security products, but they work in silos with zero interoperability.

Open platform

A secure internet gateway provides APIs and built-in integrations to easily add and share intelligence among systems.

On average, companies use more than 475 third-party applications[9]

Lack of visibility for SaaS apps

With traditional security, you have limited or zero control over sensitive data in the cloud.

Discovery for SaaS apps

A secure internet gateway helps you address risky or unsanctioned SaaS apps by easily identifying all accessed apps across an organisation.

Discover how a secure internet gateway can help your organisation protect users anywhere they access the internet.

Get the details by reading "The Rise of the Secure Internet Gateway."

Sources:

1 - "Securing Direct-To-Internet Branch Offices: Cloud-Based Security Offers Flexibility And Control," Forrester, 2015

2 - "Securing Portable Data and Applications," SANS, 2015

3 - "Keeping SaaS Secure," Gartner, 2016

4 - "Your Users Have Left the Perimeter. Are You Ready?" IDG, 2016

5 - "Visual Investigations of Command & Control Botnet Behavior," Cisco (Lancope), 2013

6 - "2015 Cost of Data Breach Study: Global Analysis," Ponemon Institute, 2015

7 - "Cisco 2017 Annual Cybersecurity Report," Cisco, 2017

8 - "The Cost of Malware Containment," Ponemon Institute, 2015

9 - "Cloud Cybersecurity Report: The Extended Perimeter," Cisco (Cloudlock), 2015