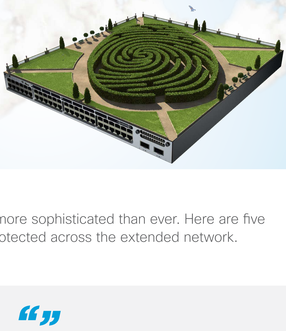
5 ways to activate network security everywhere



Threats are everywhere and more sophisticated than ever. Here are five ways Cisco keeps you protected across the extended network.

"Operators of crimeware, like ransomware, are hiring and funding professional development teams to help them make sure their tactics remain profitable."

– Cisco 2015 Midyear Security Report

1

Use the network as a sensor.

Malicious activities can hide in the floods of traditional alerts generated by your system. Cisco IOS® Flexible NetFlow technology–available on newer Cisco® switches, routers, and wireless solutions–gives you greater context and visibility so you can understand your normal traffic baseline and proactively detect suspicious behavior anywhere within your day-to-day environment.

2

Spot real threats in all the noise.

By collecting NetFlow and other sources of metadata, the Lancope StealthWatch System analyzes and documents every transaction that takes place on the network. Using this data, StealthWatch identifies anomalous behavior and signs of malicious activity.[1]

90% of companies are confident about their security policies. 54% of those have had to face public scrutiny after a breach.

– Cisco 2015 Annual Security Report

3

Keep untrusted devices out–and let the right ones in.

As your extended network grows in complexity and as more devices try to access it, the more vulnerable you become–and threats often find their way in before you even know you've been breached. Use the Cisco Identity Services Engine (ISE) for access control to shrink your attack surface so only the right devices get on the network and malicious devices stay off.

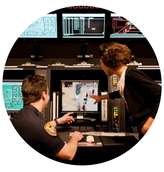
Cisco TrustSec® technology increases IT security and lowers operating cost, resulting in a 405% return on investment that pays for itself in 4.7 months.

– Forrester, *Total Economic Impact Study: Cisco TrustSec*

4

Set the rules– and enforce them.

Threats can potentially exist throughout your network. So use your network as an enforcer by employing Cisco TrustSec technology software-defined segmentation to enforce access rights consistently anywhere in the network. TrustSec interprets ISE policy to enforce the right level of access to users, prevent the lateral movement of malicious actors, and limit the impact of breaches.



"So far, 2015 is proving to be a year of unprecedented speed in the innovation, resiliency, and evasiveness of cyberattacks."

– Cisco 2015 Midyear Security Report

5

Bolster your branches.

It's hard enough to protect your campus network. Branch networks introduce a new level of complexity and greatly expand your attack surface. Cisco Intelligent WAN (IWAN) allows you to protect your extended network with the same encryption, visibility, and ease of management that you employ at your home campus. And Cisco ONE for WAN packages these advanced software capabilities together for you, making them easier to buy and deploy.

"For businesses to get the most out of their investments, security must be embedded and integrated into the entire network infrastructure."

– Kevin Phillips, director of IT operations, K&L Gates LLP

1. "Cisco & Lancope Partnership," Lancope, 2015.

© 2015 Cisco and/or its affiliates. All rights reserved. Cisco, the Cisco logo, Cisco IOS, and Cisco TrustSec are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word "partner" does not imply a partnership relationship between Cisco and any other company. (1512R)