At-a-Glance

Use the security enforcement technology already in your network to:

- Quickly isolate and contain threats across your infrastructure.
- Limit the impact of attacker infiltration by segmenting your network.
- Centrally apply granular and consistent access control across users, devices, locations, and more.

"The Cisco solution gives us a very precise way, from the wireless access point or the switch, to identify who is trying to access what. It allows us to place users in the right category and have the right policy to match information security demands."

Roman Scarabot-Mueller
Head of Infrastructure,
Mondi Group International

Cisco Network as an Enforcer

Use Network Segmentation to Contain Risks

Your network continually faces advanced cyberattacks from professional hackers at a time when Internet connections are increasing by the minute. Each network connection, whether created by cloud services, mobility, the Internet of Things (IoT), or something else, represents a potential attack entry point. Your challenge is to balance the network access that users and devices need with risk mitigation.

The good news is that your Cisco® network already contains the tools to do that. You just need to activate them to allow your network to serve as an enforcer of network security policy. For example, you can contain threats by using Cisco TrustSec® and the Cisco Identity Services Engine (ISE) to partition your network into smaller segments. Through a software-defined approach to network segmentation, you can then protect the segments using specific group policies that determine user access based on user roles and their business needs.

The result? You securely control network access that is role-based and topology- and access-independent. You greatly reduce your "attack surface." That means that even if hackers do make their way into your network, they can no longer move freely about and cause widespread damage.

Centrally Enforce Dynamic Policy

With your Cisco network acting as a network security enforcer, you centrally apply your security policies networkwide. The right users and devices now enjoy the right access, and you contain the impact of an attack. Cisco ISE serves as the centralized policy engine that provides real-time access control decisions for Cisco switches, routers, and security devices.

You can also reduce the scope, cost, and complexity of the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) network compliance audits.

Use the Cisco as a network enforcer approach to help lower security risks, improve security operational efficiency, and enhance compliance.

Next Steps

To learn more about using the Cisco Network as an Enforcer solution, visit the Cisco Enterprise Network Security page.

C45-734478-00 06/15