

Controlling who and what gets on your network

Make your workforce more productive by providing easy, highly secure mobile access anywhere.



By 2021, there will be an average of **3.5 mobile devices** per capita.*

Control access to your network and evolve to an intent-based network in four easy steps:



Step 1: Manage access policy

Is access under control?

[See more](#)



Step 2: Automate segmentation

Can you minimize risk?

[See more](#)



Step 3: Detect threats faster

Is encrypted data a growing risk?

[See more](#)



Step 4: Provide highly secure access anywhere

Can you protect mobile users?

[See more](#)

Test network readiness

[Use the DNA Advisor](#)

Step 1: Manage access policy



Ask yourself

Are you bogged down with the complexity of managing access policy across your entire network?



Something to consider

By centralizing policy management, you gain contextual awareness of everything hitting your network. Provide access consistently and efficiently while relieving the stress of complex access management.



Recommended solutions

- [Identity Services Engine \(ISE\)](#)
- [Security Services for ISE](#)

Benefits: In addition to gaining full control of all devices accessing your network, ISE allows you to apply threat intelligence so that you can contain suspicious devices fast.



Find out more

[Learn more about ISE](#)

[Back to top](#)

Did you know?

Traffic from wireless and mobile devices will account for more than 63 percent of total IP traffic by 2021.



Source: Cisco VNI Report, 2017.

Step 2: Automate segmentation



Ask yourself

Is there an easy way to reduce the risk of spreading malware by segmenting groups of employees, guests, partners, and IoT devices?



Something to consider

Due to time-consuming manual operations, many IT teams find it difficult to apply segmentation effectively. With automated policy-based segmentation, you can reduce both threats and administration overhead.



Recommended solutions

- [Cisco Software-Defined Access \(SD-Access\)](#)
- [SD-Access services](#)

Benefits: Get full control over which users have access to which resources, anywhere in your enterprise. Integrating with your existing ISE deployment, Cisco Services can help accelerate your transition to SD-Access.



Find out more

[Learn about segmentation](#)

[Back to top](#)

Did you know?

Over 25% of organizations perceive BYOD and smart devices as a high security risk.



Source: Cisco 2017 Security Capabilities Benchmark Study.

Step 3: Detect threats faster



Ask yourself

How can you gain full visibility into who is accessing which resources? And how can you detect threats or anomalies even if data is encrypted?



Something to consider

By applying advanced cognitive analytics to all data crossing your network, you can identify attacks that would otherwise go undetected.



Recommended solutions

- [Stealthwatch Enterprise](#)
- [Encrypted Traffic Analytics \(ETA\)](#)

Benefits: With intraflow telemetry captured on Catalyst 9000 switches and ISR 4000 and ASR 1000 routers, you can identify malware even in encrypted traffic, without compromising privacy. We can help you get started faster with full lifecycle services for Stealthwatch.



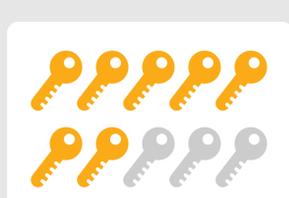
Find out more

[Download ETA white paper](#)

[Back to top](#)

Did you know?

In 2019, 70% of attacks will use encryption.



Source: Encrypted Traffic Analytics white paper, Cisco, 2018.

Step 4: Provide highly secure access anywhere



Ask yourself

How can you protect your mobile users accessing the internet from any device, from anywhere, even when they've left your corporate network?



Something to consider

By blocking malicious Internet destinations before a connection is ever established, you can prevent malware from getting on your network and can protect your users.



Recommended solutions

- [Cisco Umbrella](#)
- [Cisco AMP for Endpoints](#)
- [Cisco Security Connector for iOS](#)

Benefits: Protect users by stopping them from accessing malicious sites. Detect, block, and remediate advanced malware across all endpoints. And deepen visibility and control for iOS devices.



Find out more

[Secure branch offices](#)

[Back to top](#)

Did you know?

For enterprises, 50% believe that their mobile infrastructure is at a high risk for a security breach.



Source: Security Risk and Trustworthiness Study, Cisco, 2017.

Test network readiness

[Use the DNA Advisor](#)

Transform to an intent-based network with Cisco DNA

* Source: Cisco VNI Report 2016