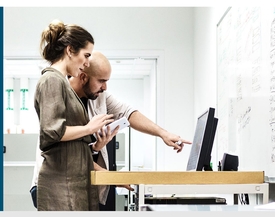
Identifying and containing threats fast

Minimize risk and ensure compliance by identifying threats on your network fast.



On average it takes **191 days** to uncover a breach.*

Address your concerns for network threats and evolve to an intent-based network in four easy steps:

Step 1: Gain visibility

Are you able to detect threats fast?

See more

Step 2: Detect encrypted threats

Can you identify encrypted threats?

See more

Step 3: Contain threats

Can you stop breaches fast?

See more

Step 4: Secure the perimeter

Are your firewalls able to cope?

See more

Protect against threats

Read annual cybersecurity report

Step 1: Gain visibility

Ask yourself
Do you have clear visibility and insights into threats and attacks on your network?

Something to consider
By using telemetry from existing network infrastructure for advanced threat detection, as well as deep forensics, you can outsmart emerging threats in your network.

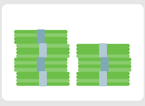
Recommended solutions
- Network as a Sensor
- Cisco Security Stealthwatch Deployment Service

Benefits: Turn your entire network into a sensor for threats and attacks. You can identify attacks in near real time, while reducing false positives and operations time.

Find out more

Learn about Stealthwatch

Did you know?
The average cost of a data breach is $3.62 million.



Source: 2017 Cost of Data Breach Study, Ponemon Institute.

Back to top

Step 2: Detect encrypted threats

Ask yourself
Do you have visibility into the growing number of encrypted attacks on campus and at branches?

Something to consider
When you can identify threats in encrypted traffic without decrypting them, you can protect your business without compromising privacy.

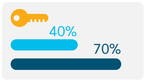
Recommended solution
- Encrypted Traffic Analytics

Benefits: Gain visibility and insight into potential threats in encrypted traffic.

Find out more

Learn what Enterprise Network Security can do for you

Did you know?
40% of traffic is encrypted, and that number is growing. In 2019, 70% of attacks will use encryption.



Source: Gartner, Security Leaders Must Address Threats from Rising SSL Traffic, Jeremy D'Hoinne, Adam Hils, 2013.

Back to top

Step 3: Contain threats

Ask yourself
Is it challenging to quickly contain threats once they have been identified on your network?

Something to consider
You can protect against potential IoT attacks by blending a security architecture with security services. Defend your IoT devices and keep your business running.

Recommended solutions
- Cisco Identity Services Engine (ISE)
- Rapid Threat Containment

Benefits: Cisco ISE and Stealthwatch Enterprise help IT mitigate security issues before they become events that can incur significant remediation time and cost.

Find out more

Get Forrester research

Did you know?
Nearly half of the security risk that organizations face stems from having multiple security vendors and products.

Source: Cisco Annual 2018 Cybersecurity Report.

Back to top

Step 4: Secure the perimeter

Ask yourself
How well can you identify sophisticated threats at the edges of your network?

Something to consider
By deploying next-generation firewalls, you gain a contextual view of all users and applications at the edges (Internet and WAN).

Recommended solutions
- Firepower NGFW with NGIPS and AMP
- Security Implementation Services

Benefits: Get superior visibility, embedded security intelligence, automated analysis, and industry-leading threat detection. Increase the value of your solutions while reducing downtime with our implementation services.

Find out more

Request a free trial

Did you know?
Attackers can infect 100,000 IoT devices in 24 hours.

Source: Cisco 2017 Midyear Cybersecurity Report.

Back to top

Protect against threats

Read annual cybersecurity report

Transform to an intent-based network with Cisco DNA

* Source: 2017 Cost of Data Breach Study, Ponemon Institute.