Top 5 Reasons Why Cisco Leads the Industry in NGIPS

Cisco Firepower NGIPS provides network visibility, threat intelligence, automation and industry leading threat effectiveness. Gartner has ranked Firepower NGIPS as a Magic Quadrant Leader for seven years running, and the independent NSS Labs testing organization consistently rates it as a "Recommended" IPS solution for eight years.

It is important to understand how Firepower NGIPS is different from other vendors and how that differentiation can help your organization. The business impact is significant allowing a number of unique benefits which improve the security posture of your enterprise:

1 | Visibility

Cisco Firepower NGIPS can see what other solutions cannot.

Utilize Firepower Management Center as your centralized security console to see more contextual data from your network. This allows you to fine tune your security that is specific to the needs of your organization. View applications, indications of compromise, host profiles, file trajectory, sandboxing, vulnerability information and device level OS visibility. See more of your network by using these data inputs to optimize your security through policy recommendations or Snort customizations.

2 | Efficacy

NGIPS gets pushed new policy rules and signatures every two hours ensuring your security is always up to date.

Cisco security intelligence, Talos, brings security effectiveness to every Cisco security product by leveraging the largest threat detection network in the world. This industry leading threat intelligence works as an early warning system which constantly updates with new threats.

3 | Operational cost

NGIPS increases operational effectiveness.

Help your staff achieve more by automatically prioritizing the threats that matter and improve your security through policy recommendations based on your network's vulnerabilities. Use NGIPS automation to separate actionable events from noise creating greater operational efficiency while reducing overhead. Automatically get informed as to which rules to activate/deactivate and filter events pertinent for the devices on your network.

Resources

Protecting Your Digital Business: The Case for Next-Generation Intrusion Prevention

Find out why adding an NGIPS to your security architecture is advantageous.

Read White Paper

What Is NGIPS?

Learn the distinct advantage a Cisco Firepower NGIPS delivers to your Network Security efforts.

Watch the video

Cisco NGIPS Website

Stay up-to-date on the latest trends and see what's new in security from Cisco.

Learn More

Effective Security: Network. Endpoint. Cloud.

Visit www.cisco.com/go/ngips

Follow us on Twitter
@CiscoSecurity

4 | Flexibility

Cisco Firepower NGIPS flexible deployment options meets the needs of the enterprise.

It can be deployed at the perimeter, data center distribution/ core, or behind firewall to inspect both north-south and east-west traffic to protect mission critical assets, guest access, WAN connections, etc. NGIPS can be deployed for inline inspection, or passive detection.

5 | Integration

Customers are choosing Cisco Security solutions due to the open architecture and feature integration.

Firepower NGIPS plugs into what you already have in your network without major hardware changes or significant time to implement. Enable and manage several security applications from a single pane of glass with Firepower Management Center. Seamlessly navigate between NGIPS, NGFW and AMP to optimize your security policies as well as have the ability to ingest 3rd party intelligence via Cisco Threat Intelligence Director.