Cisco Security ASA with FirePOWER Services—Sales Battle Card

Protect your customers—and advance your security offering.

Cisco ASA with FirePOWER Services is the industry's first adaptive, threat-focused next-generation firewall (NGFW) designed for a new era of threat and advanced malware protection. Cisco ASA with FirePOWER Services delivers integrated threat defense for the entire attack continuum—before, during and after an attack. It combines the proven security capabilities of the Cisco ASA firewall with industry-leading Sourcefire threat and advanced malware protection in a single device. The solution uniquely extends the capabilities of the Cisco ASA 5500-X Series beyond what other NGFW solutions are capable of.

What sets it apart?

Cisco ASA with FirePOWER Services offers a unique and comprehensive solution for network security based on Cisco's threat-centric security model—designed to address the complexities of today's network environment and the challenges security administrators face today.

- Provides full-stack threat visibility from physical layer to application layer, from attacker to target
- Integrates and delivers NGFW, Next-Generation Intrusion Prevention System (NGIPS) and AMP in the core product without the need for a separate client agent or to add another product to the NGFW
- Has enough context to accurately and dynamically adapt security controls to a changing network and send out impact flags to alert the SecOps team to the most critical threats
- Automatically adapts defense to dynamic changes in the network
- Incorporates the industry's leading IPS detection technologies and Advanced Malware Protection (AMP) effectiveness as proven by NSS Labs
- Delivers the industry's highest catch rate against malware URLs
- Offers total network visibility

TARGET BUYER	WHAT THEY CARE ABOUT:
CSO	• Reducing risk and enabling innovation • Protecting intellectual property/ data assets • Meeting regulatory requirements • Improving operational efficiency
CIO	• Keeping systems running • Facilitating business flexibility • Meeting regulatory requirements • Coping with personnel/budget constraints
CHIEF SECURITY ARCHTECT	• Developing effective security architecture • Setting and enforcing policies • Meeting regulatory requirements • Monitoring evolving security landscape
SECURITY OPERATIONS	• Addressing and reducing risk • Managing disparate point products • Coping with personnel/budget constraints • Eliminating security blind spots
NETWORK OPERATIONS	• Keeping the network running/performing well • Balancing user demands with budget/ space limitations • Reducing network impact of security • Simplifying management

BUYER CONVERSATIONS

Challenge 1: Lack of visibility into threats	Challenge 2: Need to remediate advanced malware and threats	Challenge 3: Efficiently and cost-effectively manage security infrastructure
You lack the visibility into what you're protecting on your network, making threat detection and response less effective.	You're unable to detect and quickly remediate today's more advanced malware threats.	The complexity of managing your security infrastructure has driven up costs and limited its effectiveness.
How this affects you Without a clear understanding of your vulnerabilities and real-time contextual awareness, it's nearly impossible to protect your dynamic network and organization's assets from sophisticated threats and prioritize a response.	**How this affects you** If you're unable to detect emerging and advanced threats early, then you won't be aware of the damage they cause and will incur higher cleanup costs.	**How this affects you** Adding point solutions for each new security challenge increases complexity, wastes management resources, and leaves gaps in security defenses that are entry points for exploitation.
What if you could... Get comprehensive, real-time visibility into users, infrastructure, applications and content to help detect sophisticated threats and automate responses.	**What if you could...** More readily detect breaches as they happen and more quickly remediate successful breaches.	**What if you could...** Deploy an integrated threat defense solution that reduces operating costs and administrative complexity and easily integrates with your existing IT environment, work stream and network fabric.
With Cisco you can! Passively discover everything you need to protect and the critical threats you're facing so you can invoke tailored threat detection policies to optimize security effectiveness.	**With Cisco you can!** Get integrated threat defense to discover, understand and stop malware and emerging threats missed by other security layers.	**With Cisco you can!** Cisco ASA with FirePOWER Services delivers integrated threat defense for the entire attack continuum in a single device. This reduces complexity and cost, streamlines operations and provides superior threat protection.

How Ingram Micro can help

Ingram Micro's focus on security has never been stronger. Our team can help you with ESS Security specialization; business, sales and technical training opportunities; Cisco Services; and Ingram Micro Professional Services support. We have the largest team in the industry, with 150 experts able to assist you with vertical markets, certification levels and regional support, as well as sales, technical support and marketing.

Contact us today:

Collin Rauen, Channel Account Specialist
collin.rauen@ingrammicro.com
(800) 456-8000, ext. 66092

For more information on
Cisco Security, please visit:
http://www.ingrammicroadvisor.com/cisco/resources/security