Cisco Expo
2012

Securing Your Web Communication

T-SECB1&2

Hrvoje Dogan, Consulting Systems Engineer, Security

© 2012 Cisco and/or its affiliates. All rights reserved.

Prosíme, ptejte se nás

- Twitter www.twitter.com/CiscoCZ
- Talk2cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco Web Security Portfolio

Web Security Appliance
(WSA)

ScanSafe

THREAT DEFENSE
Block Malware
Prevent Data Loss

ACCEPTABLE USE ENFORCEMENT
Application Control visibility
URL Filtering

Centralized Management and Reporting

Coffee Shop

Home Office

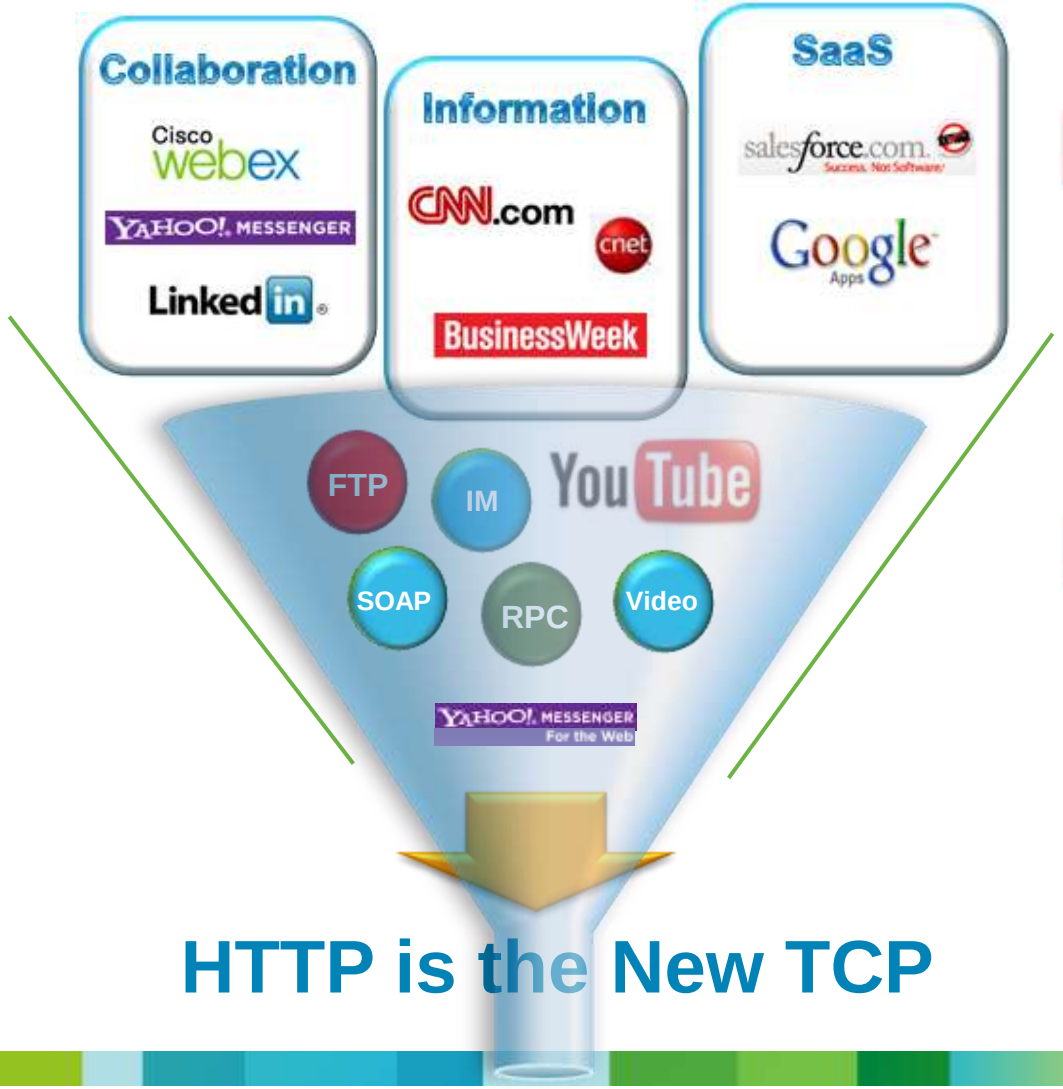
Mobile User

AnyConnect Secure Mobility

© 2011 Cisco and/or its affiliates. All rights reserved.

Increasing Enterprise Web Traffic

Ubiquitous Path In and Out of Enterprise Networks



- Growing business web usage
- Growing tunneled apps usage

HTTP is the New TCP

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Security Appliance

Adressing Business Challenges

Secure

Against Malware

Cisco IronPort S-Series

Prevent

Data Breaches

Control

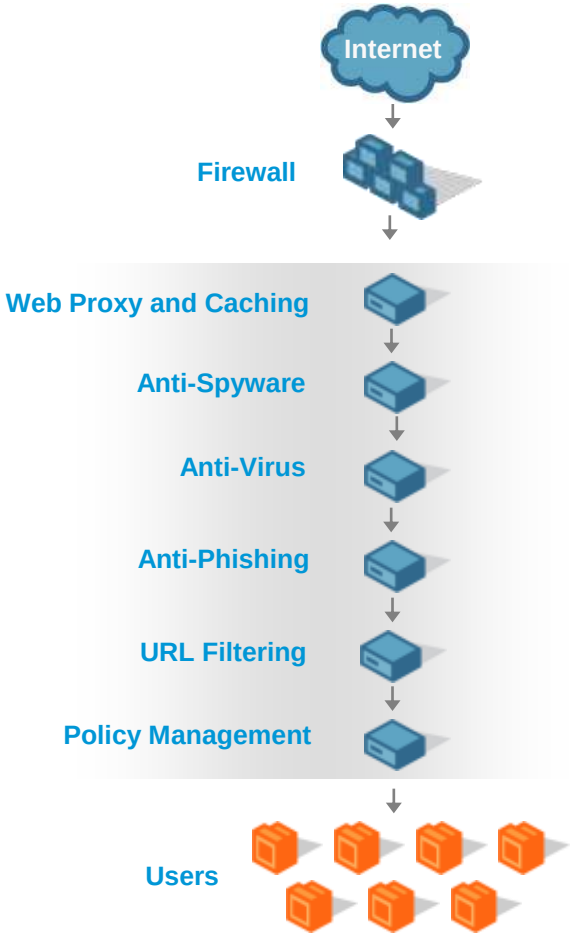
Web Traffic and Applications

© 2010 Cisco and/or its affiliates. All rights reserved.

Next-Generation Secure Web Gateway

Consolidation Drives Operational Efficiency

Before Cisco IronPort



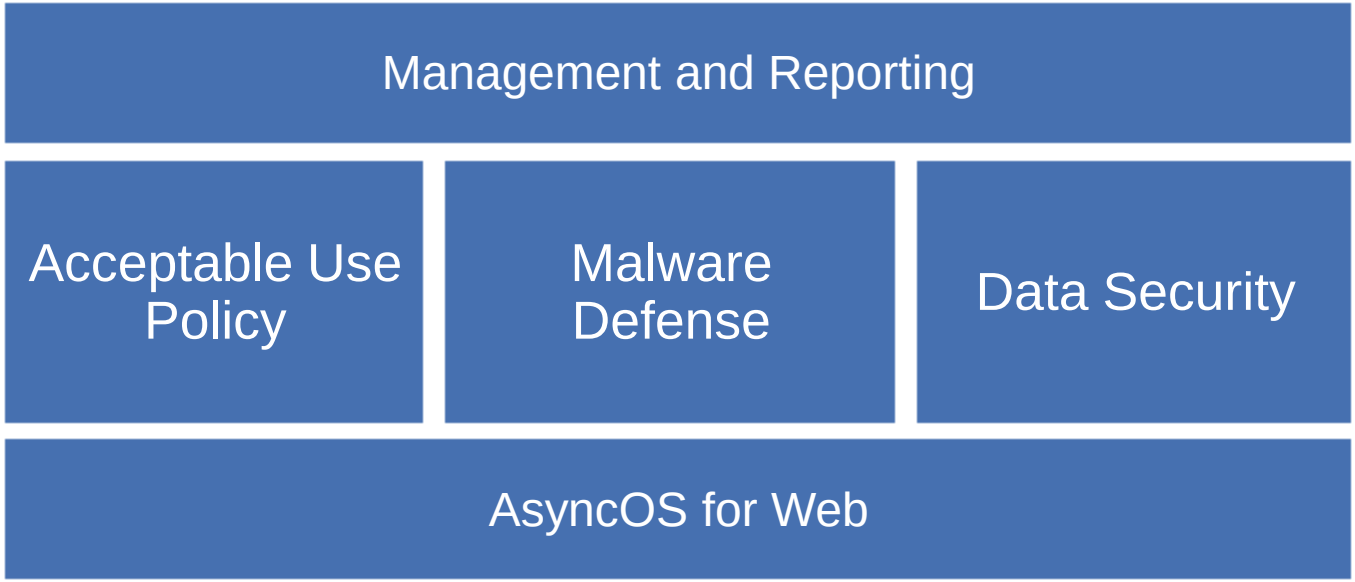
After Cisco IronPort

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Security Appliance

A Powerful, Secure Web Gateway Solution

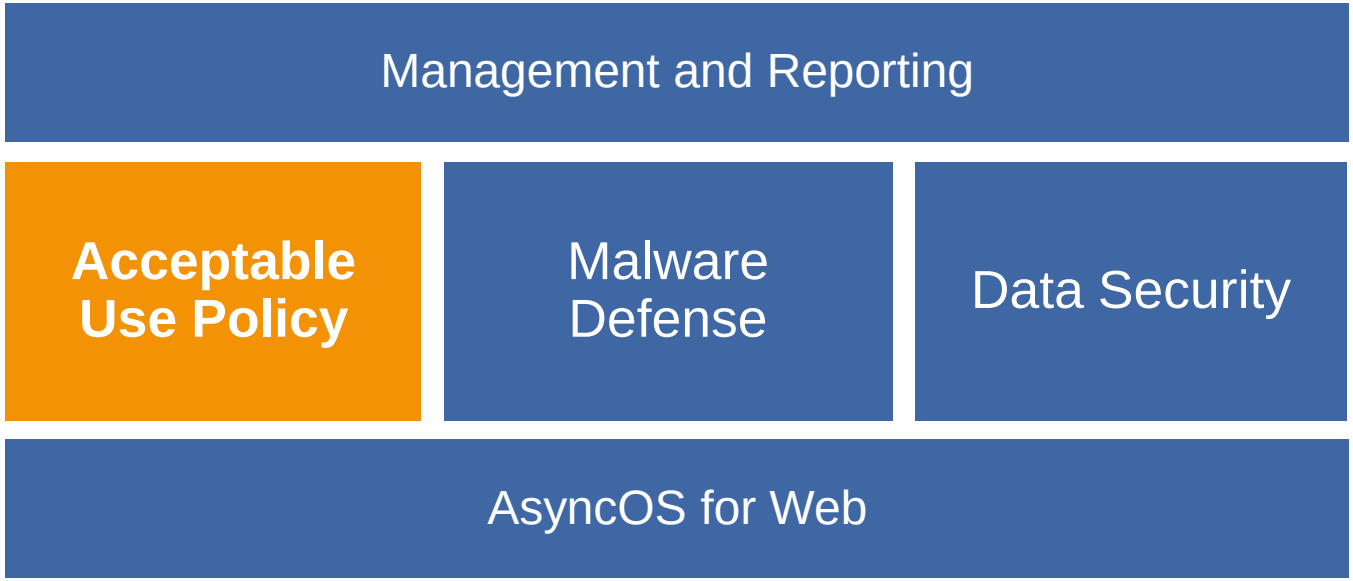
- Most effective defense against web-based malware
- Visibility and control for acceptable use and data loss
- High performance to ensure best end-user experience
- Integrated solution offering optimum TCO



© 2011 Cisco and/or its affiliates. All rights reserved.

Acceptable Use Enforcement

Visibility and Control for the Web and Web Applications



- Enterprise-class URL filtering
- Applications and object filtering
- Integrated identity and authentication

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Usage Controls
Leading Efficacy, Rich Controls, Comprehensive Visibility

Control

- Per user, per group policies
- Multiple actions: block, warn, monitor
- Time-based policies
- Unlimited custom categories
- Custom end-user notifications

Visibility

- Easy to understand reports
- Extensive logging
- Comprehensive alerting

Efficacy

- 200+ countries
- 50+ languages
- 65 categories
- Less than 1 in 1 million false positives

© 2011 Cisco and/or its affiliates. All rights reserved.

Application Visibility and Control

Access Control Policy

Instant Messaging
Facebook: Limited Apps
Video: 512 kbps max

Access Control Violation

File Transfer over IM
Facebook Chat, Email
P2P

- Granular control over HTTP, HTTP(s), FTP applications
- Dynamic signature updates maintained by Cisco SIO

Employee in Finance

flickr YouTube BitTorrent

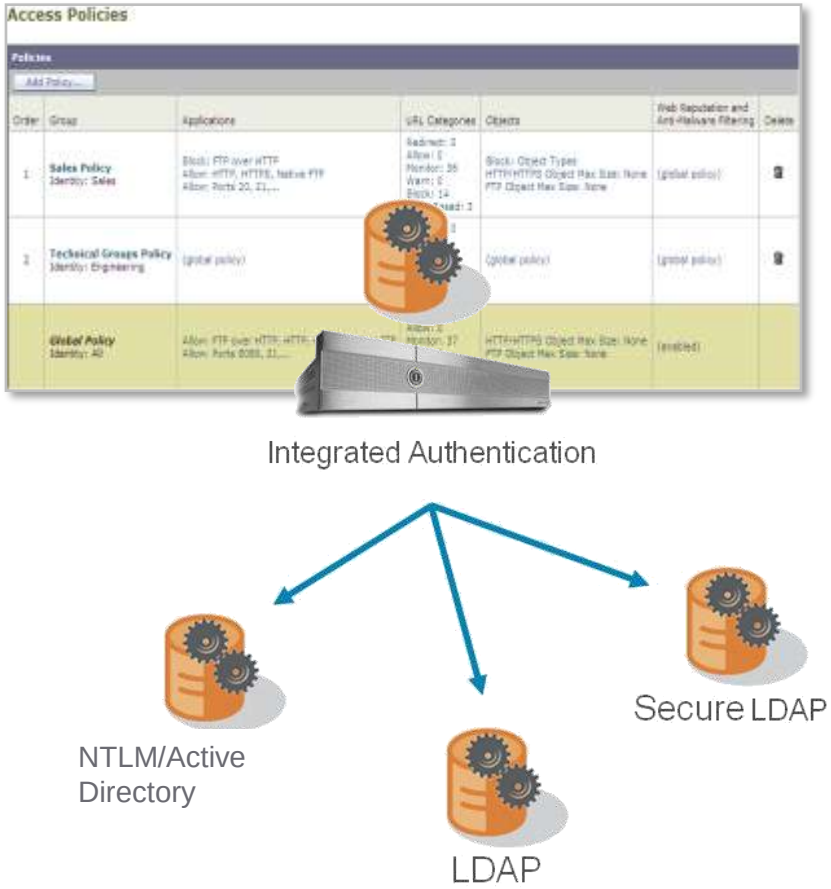
Granular Control over Application Usage

© 2011 Cisco and/or its affiliates. All rights reserved.

Integrated Identity and Authentication

User-Specific Acceptable Use and Data Security Policies

- Authentication against LDAP servers
- Transparent, single sign-on (SSO) authentication against Active Directory
- Multi-realm sequencing
- Multi-domain authentication
- Guest policies
- Re-Auth and Failed Auth policies

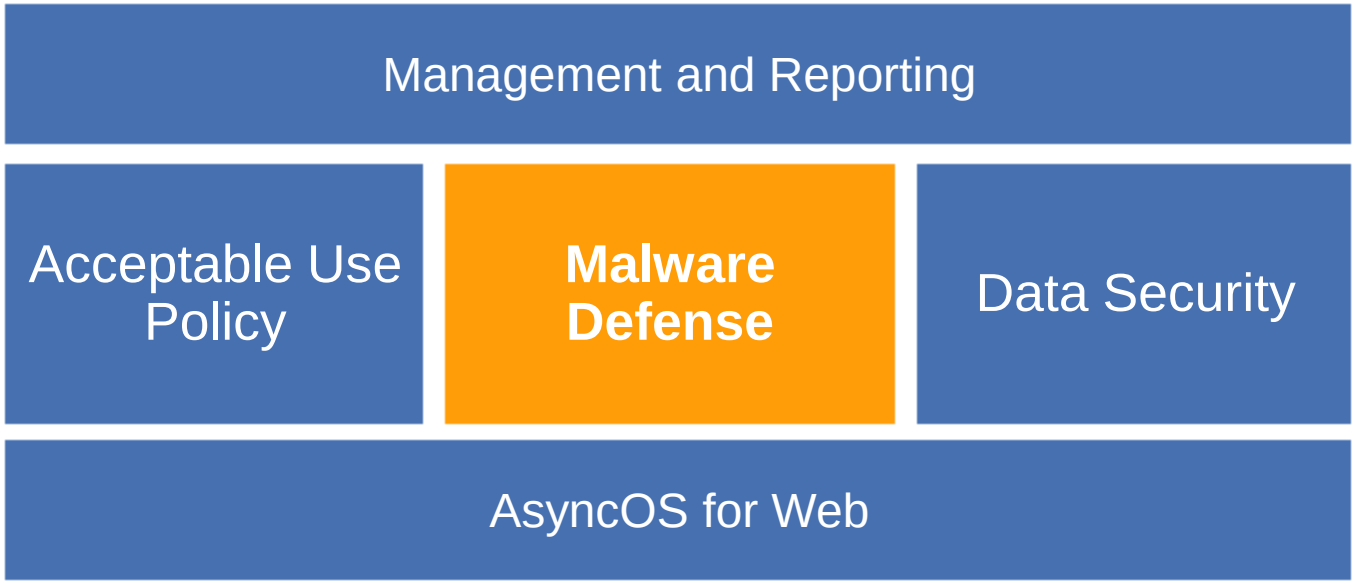


Define Acceptable Use and Data Security Policies using Rich Identity Constructs

© 2011 Cisco and/or its affiliates. All rights reserved.

Malware Defense

Multiple layers for Malware and Spyware Protection



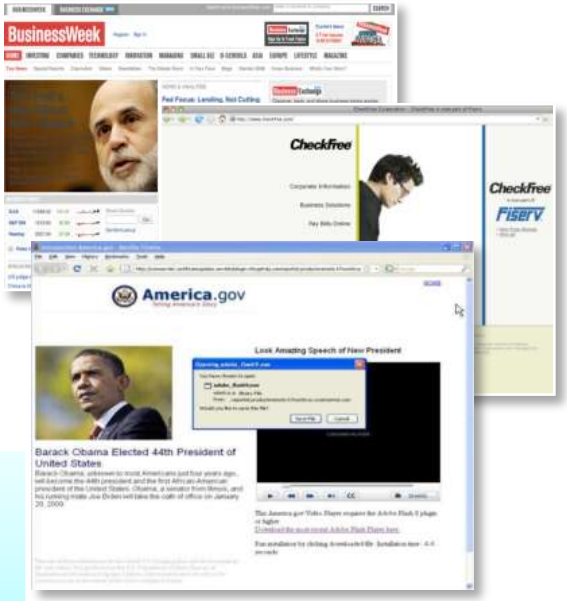
- Malware landscape
- Multi-layered malware defense
- Network layer phone-home prevention
- Reputation filtering and signature scanning

© 2011 Cisco and/or its affiliates. All rights reserved.

Multi-Layered Malware Defense

Protection Against Today's Threats

Layer 4 Traffic Monitor → Web Reputation Filters → Dynamic Vectoring and Streaming Engine



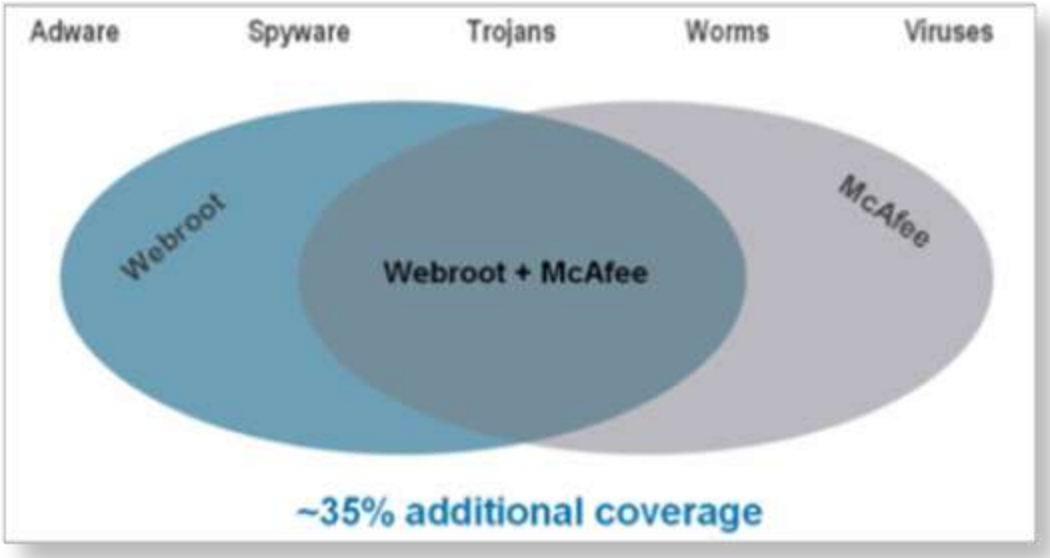
- Detects malicious botnet traffic across all ports
- Blocks 70 percent of known and unknown malware traffic at connection time\
- Blocks malware based on deep content analysis

© 2011 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort DVS Engine

Dynamic Vectoring and Streaming

- Accelerated signature scanning
  - Parallel scans
  - Stream scanning
- Multiple integrated verdict engines
  - McAfee, Webroot and Sophos
- Automated updates
- Decrypt and scan SSL traffic
  - Selectively, based on category and reputation



© 2011 Cisco and/or its affiliates. All rights reserved.

AnyConnect Secure Mobility

Anytime, Anywhere Secure Access With WSA

Cisco Security Enforcement Array (SEA)

1 Cisco AnyConnect 2.5/3.0

Always-on, location-aware, extremely lightweight, invisible to user

Supported on all major devices and OS

2 Powerful Enforcement Engines

High Performance

Application and Identity Aware

Hybrid Hosted Delivery

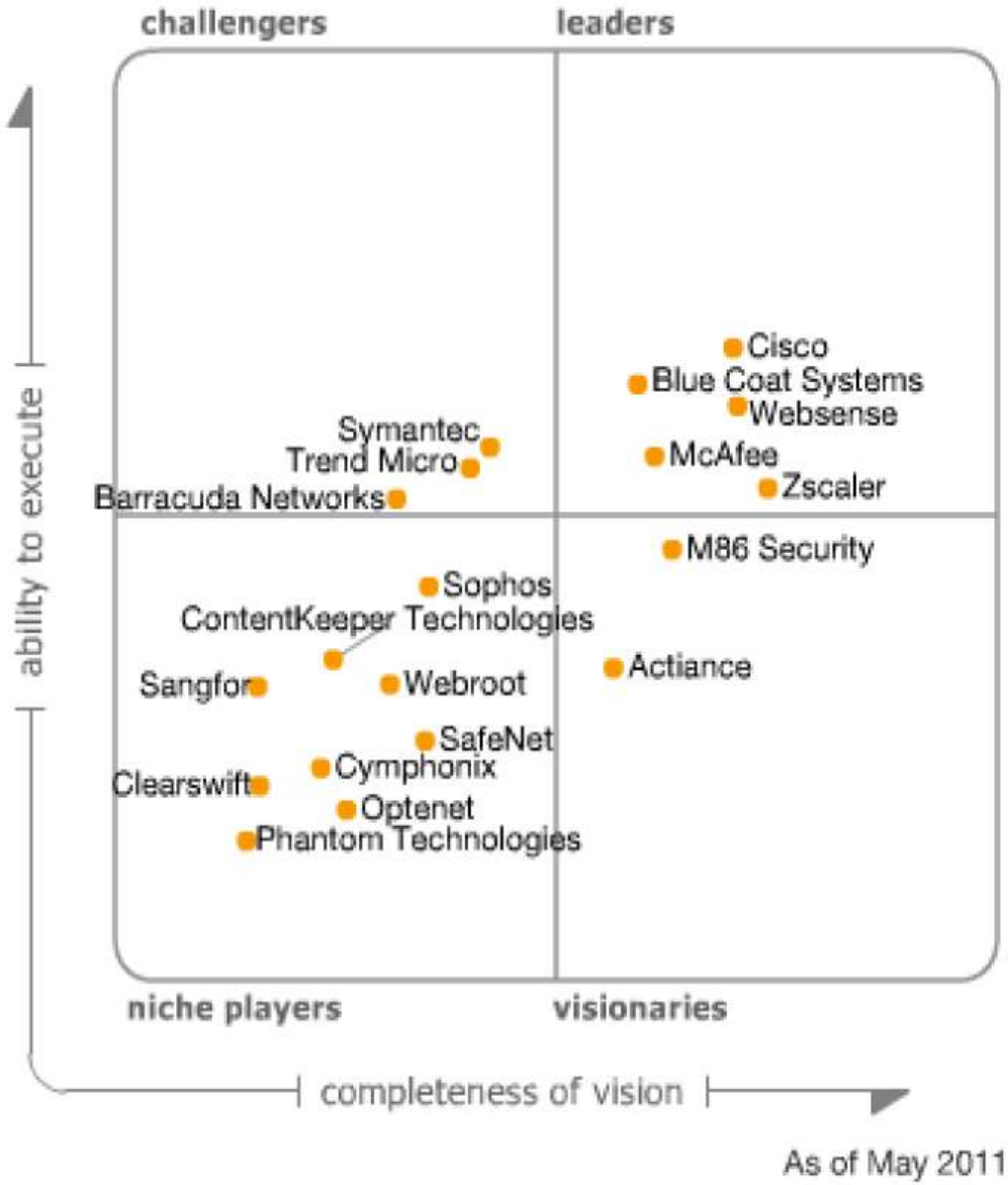
3 Policy

Abstracted from enforcement layer

Acceptable Use, Access Control, Data Security, Anti-Malware

© 2011 Cisco and/or its affiliates. All rights reserved.

Gartner Magic Quadrant for *Secure Web Gateway, 2011*



Source: Gartner (May 2011)

The Magic Quadrant is copyrighted 2011 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Cisco.

© 2011 Cisco and/or its affiliates. All rights reserved.

Otázky a odpovědi

- Twitter www.twitter.com/CiscoCZ
- Talk2Cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

- Zveme Vás na **Ptali jste se…** v sále **LEO**
  1.den 17:45 – 18:30
  2.den 16:30 – 17:00

© 2011 Cisco and/or its affiliates. All rights reserved.

Prosíme, ohodnoťte tuto přednášku.

© 2011 Cisco and/or its affiliates. All rights reserved.

CISCO