



Appliance di Sicurezza da Symantec

Infosecurity



Alessandro Gioso – Principal System Engineer
10 Maggio 2006

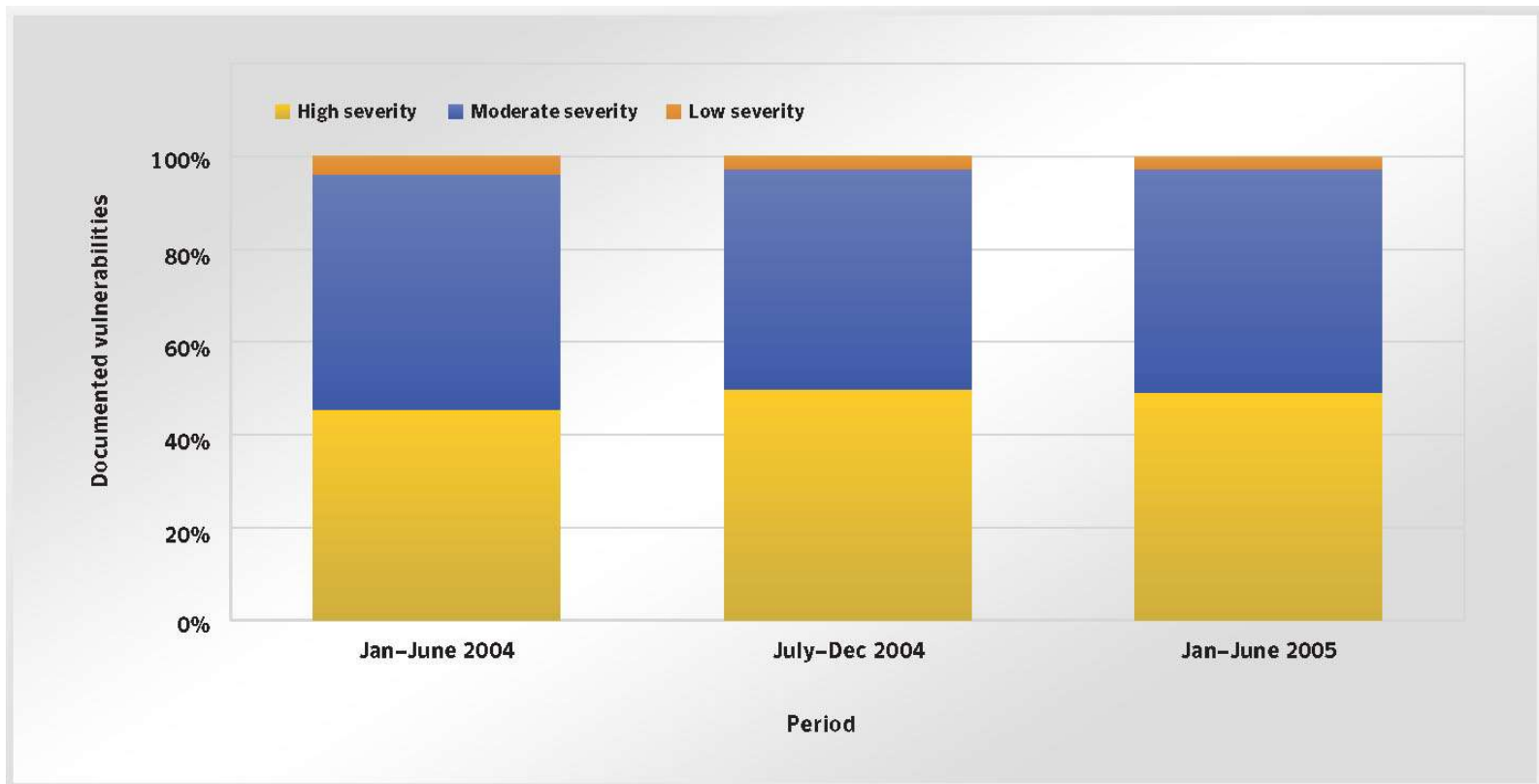


Agenda

- 1 Minacce
- 2 Soluzioni
- 3 Business case

Vulnerability Trends – Severity & Ease of Exploitation

- › 97% delle vulnerabilità documentate da Symantec erano classificate High o Moderate Severity e 84% erano utilizzabili.
- › 73% del totale delle vulnerabilità erano classificate come facili da attuare .





Unified Threat Management

- I prodotti devono unificare e integrare multiple funzioni di sicurezza in un singolo hardware (IDC)
 - Firewall
 - Network intrusion detection
 - Network intrusion prevention
 - Gateway antivirus
- } Intrusion Protection

Perche?

- Solo con prodotti flessibili e con molteplici livelli di controllo è possibile bloccare Blended threats

Threat Management

- Clienti necessitano di una combinazione di tecnologie di sicurezza per proteggersi contro blended threats
- Ogni componente di sicurezza viene sviluppato, configurato e gestito separatamente.
- Nuove tecnologie immettono nuovi rischi
 - Mobile phone
 - Instant Messenger

Customer Needs

- Riduzione di complessità e costo di
 - Acquisizione
 - Installazione
 - Configurazione
 - Management
- Protezione proattiva “zero-day”
 - Protezione contro la complessità giornaliera dei blended threats
- Soluzioni scalabili
 - Gestione centralizzata di apparati locali e remoti
 - Centralizzazione di logging, alerting, e reporting
- Modelli di licenziamento software e hardware flessibili
 - Comprare solo quello che serve oggi, espandi domani

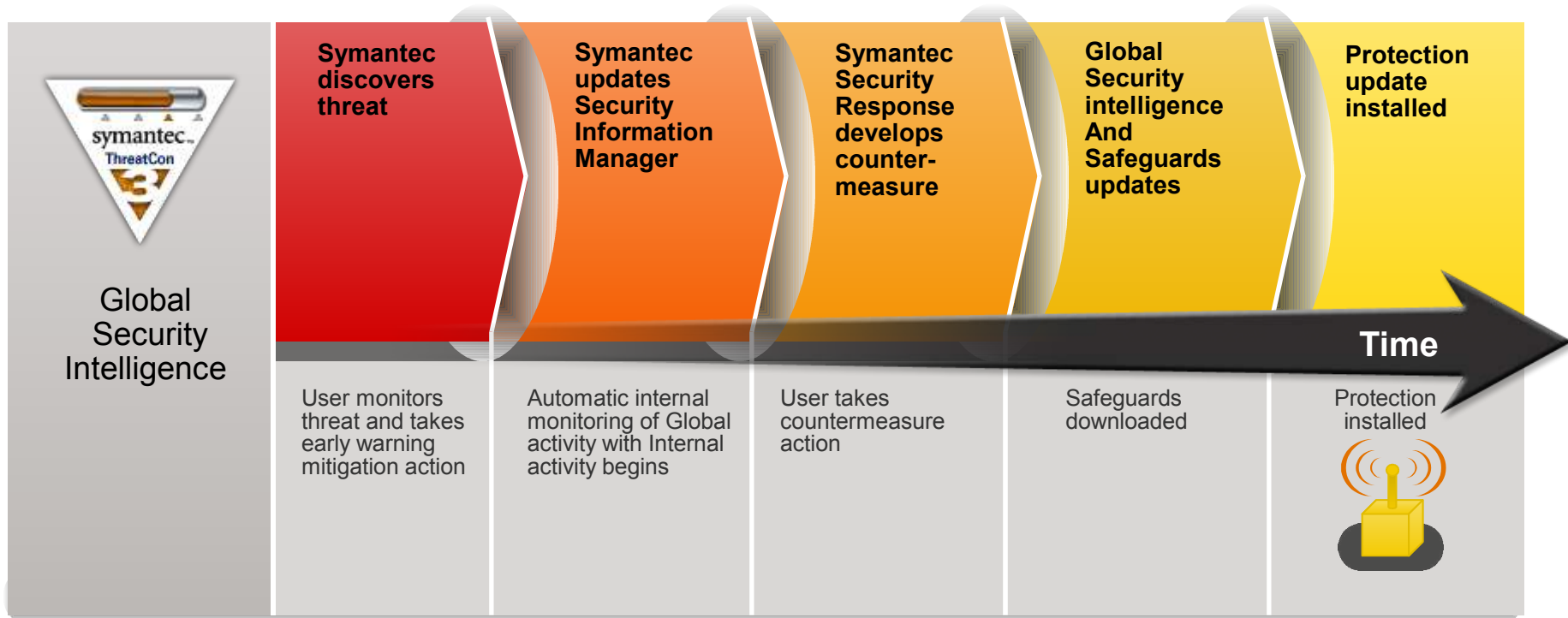
Symantec Gateway Security

- Riduzione dei costi di *acquisizione e installazione*
 - Integrazione di 7 funzioni di sicurezza in un appliance
- Sicurezza integrata a tutti i livelli
 - Rilascio di protezione proattiva per l'impresa
- Alta affidabilità
 - Facilità e riduzione dei costi HA/LB di tutte le funzioni di sicurezza integrate nell'appliance.
- Riduzione dei costi di *configurazione e management*
 - Tutte le funzioni sono gestite da una unica console
- Flessibile licensing
 - Compri quello che serve oggi ed espandi domani (funzioni e/o nodi)
- Unico Fornitore

Key Features

- Le tecnologie strettamente integrate forniscono l'efficacia massima di sicurezza e riducono i costi dell'installazione e di acquisizione
 - Full-inspection firewall
 - Award-winning virus protection
 - Intrusion prevention
 - Antispam
 - Intrusion detection
 - URL-based content filtering with Dynamic Document Review
 - IPsec and SSL VPN technologies
 - Antispyware

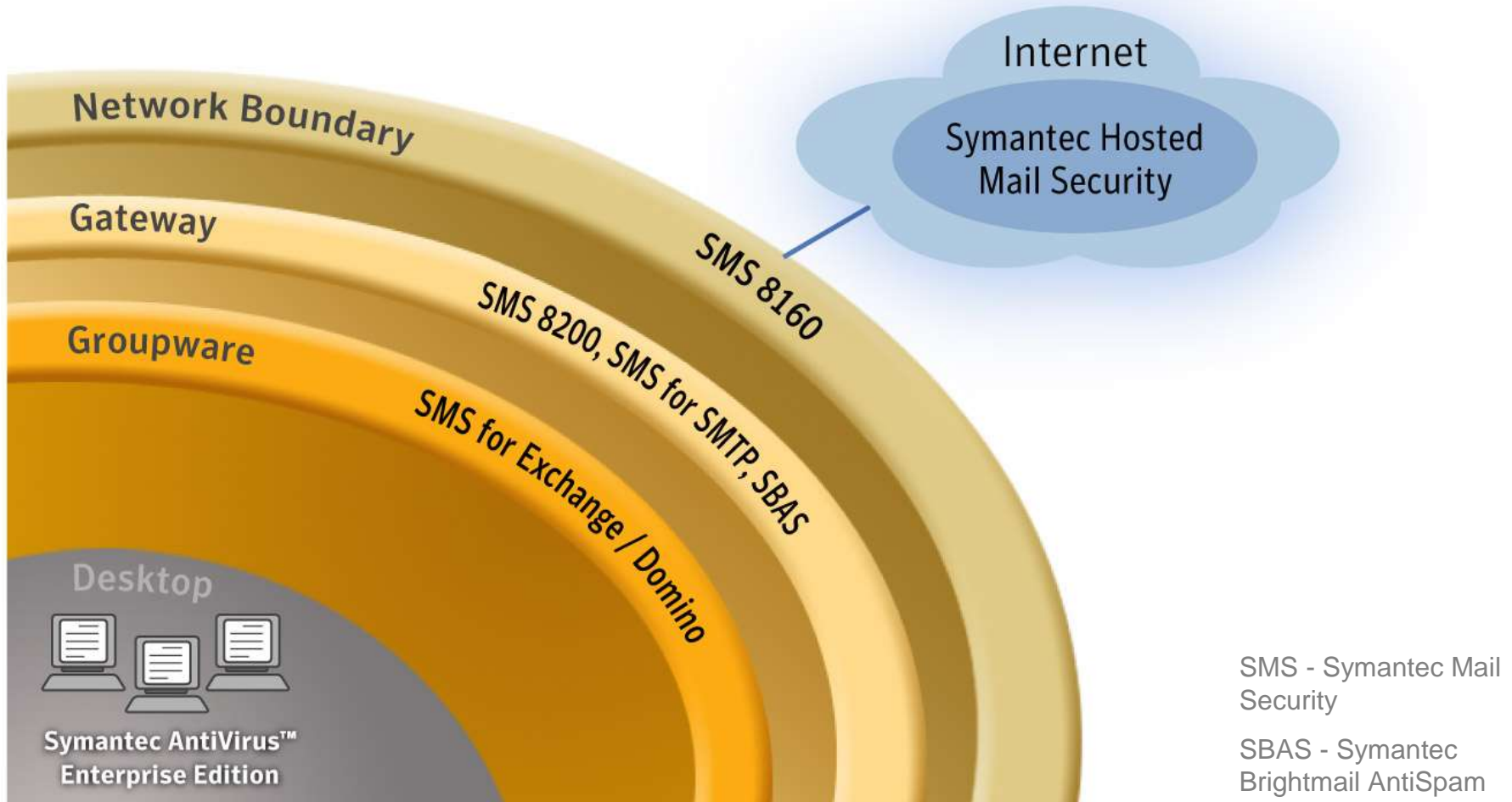
Proactive Early Warning Advantage



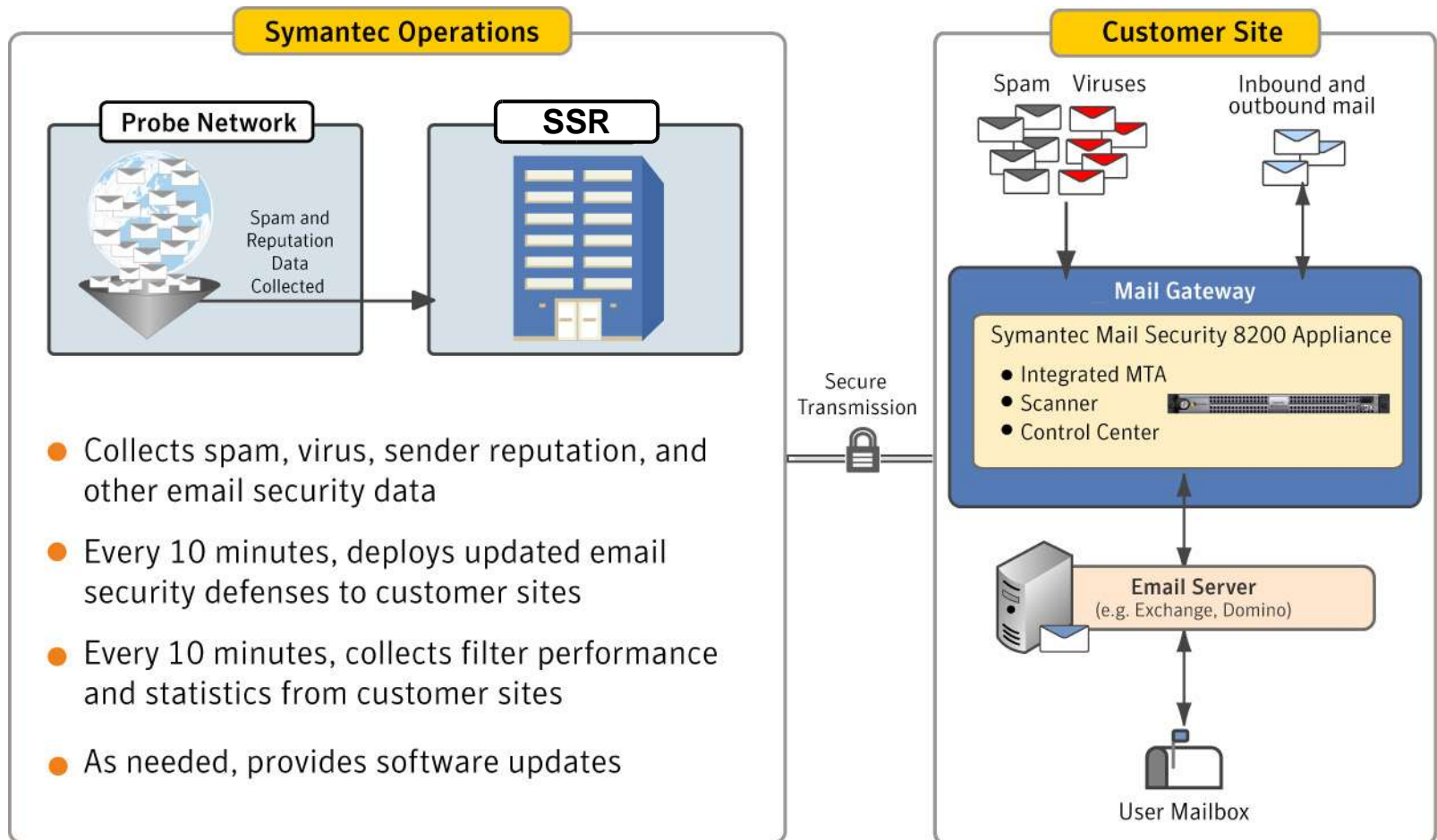
Symantec Gateway Security Series Appliances and Unified Threat Management

- Le tecnologie di sicurezza integrate permettono di ottenere la massima sicurezza effettiva
- Multiple tecnologie in un appliance riducono i costi di acquisizione e installazione
- Singola console permette completa amministrazione di tutte le tecnologie per semplificare il network security management, e riduce i costi di configurazione e management
- Combina multiple detection technologies per identificare e bloccare sia conosciuti che sconosciuti (“zero day”) attacks e worms
- Protocol anomaly detection e vulnerability attack interception
- Rilascio automatico di security content updates via Symantec LiveUpdate™ technology

Multi-layered email protection



High-level architecture



Symantec Mail Security 8200 Series Features

Appliance Form Factor

- Hardware
- Hardened Operating System
- Hardened Mail Relay

Threat Protection

- Email Firewall — Directory Harvest Attack
- Email Firewall — Spam and Virus Attacks
- Email Firewall — Global Reputation Lists
- AntiSpam Filtering – Brightmail AntiSpam
- AntiVirus Filtering – Symantec AntiVirus
- Content Filtering — Attachment Mgmt
- Content Filtering — Annotations
- Content Filtering — Archiving
- Content Filtering — Dictionaries
- Content Filtering — Custom Rule Editor
- Message Integrity – Anti-forgery via SPF
- Message Integrity – TLS Encryption

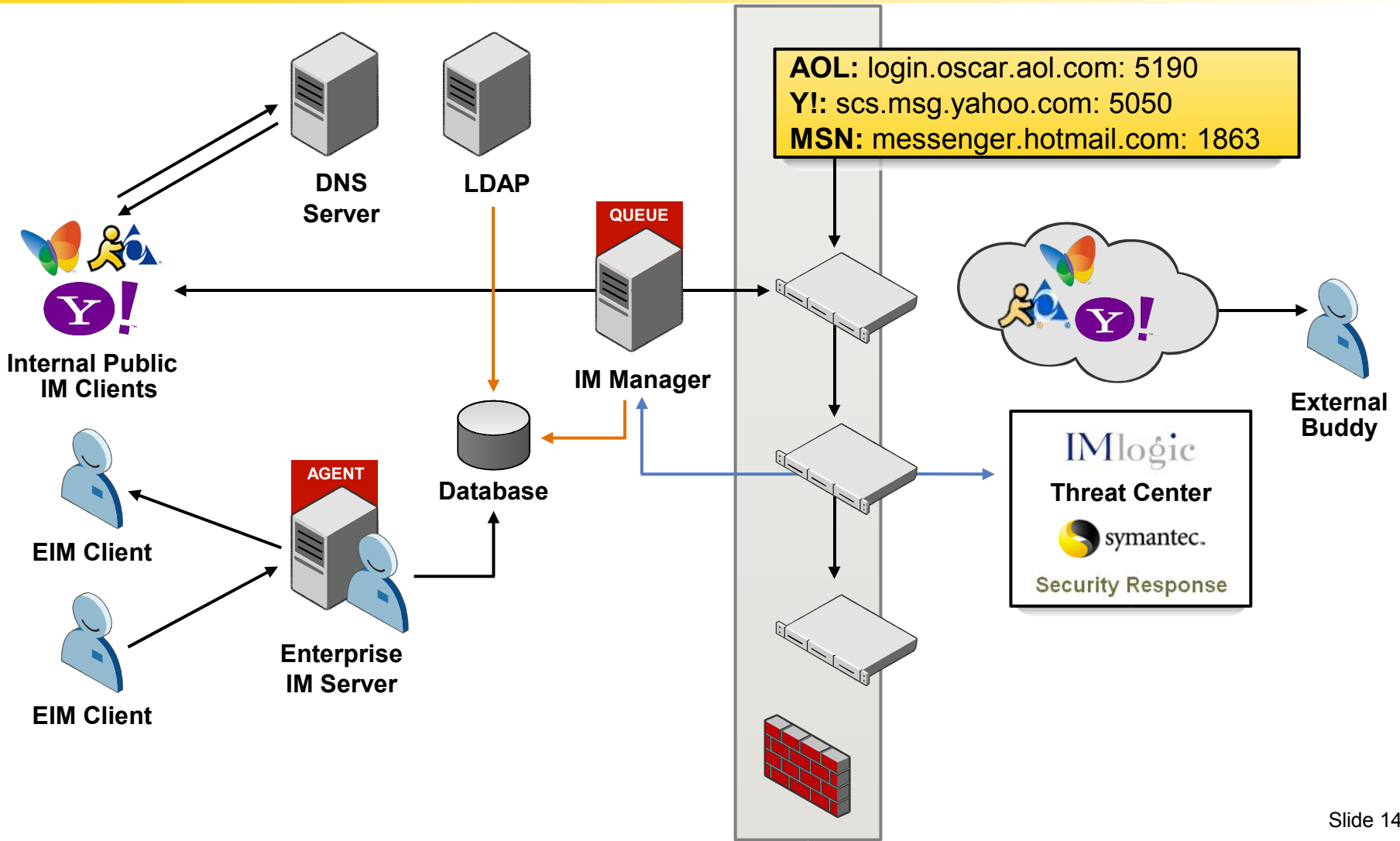
Mail Management

- Group Policies
- Outbound Policies
- LDAP Group Policies
- 16 Actions (8 New)
- Compound Actions
- End User Preferences — Block/allow list
- End User Preferences — Language
- Administrator & End User Quarantine

System Management

- Web-based Administration
- Global Management
- Multiple Administrator Roles
- Alerts
- Automatic Rule Updates
- 55 Reports (35 New)
- Software Update Mechanism

Securing Real-Time Communications: A Logical Deployment Architecture



Symantec Network Security 7100 Series



Proactive intrusion prevention device protegge contro attacchi sconosciuti e conosciuti .

- Symantec's appliance solution
 - Highly secure
 - Highly flexible
 - Scalable centralized management
 - 3 modelli per una suit enterprise network
 - Facile da installare
- Intrusion prevention appliance per sicurizzare critical networks
 - Proattiva intrusion prevention e detection
 - IMUNE* protection architecture
 - Policy Management
 - Analisi delle minacce in Real-time
 - Management Centralizzata
 - Bassa manutenzione e protezione interna con AutoProtect

*Intrusion Mitigation Unified Network Engine

Symantec Security Information Manager 9500 Series



Security Intelligence

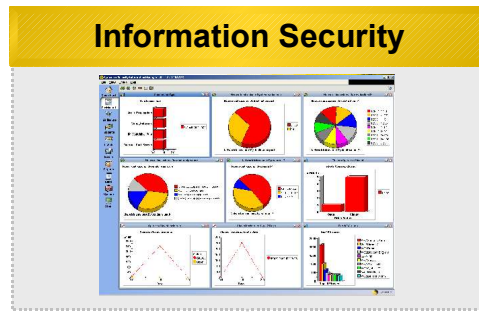
- Prima integrazione di security intelligence (DeepSight)
- Flessibile, multi-user security dashboard & compliance reports
- Incident priorities based on BIA asset criticality & vulnerability

Scalability

- High-speed appliance
- Dynamic, motore di correlazione brevettato
- Multi-tier event processing (filtering/aggregation)

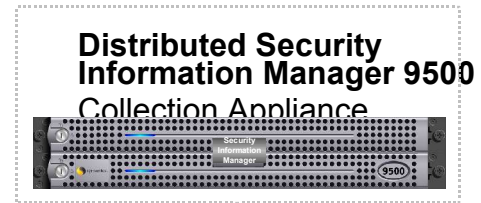
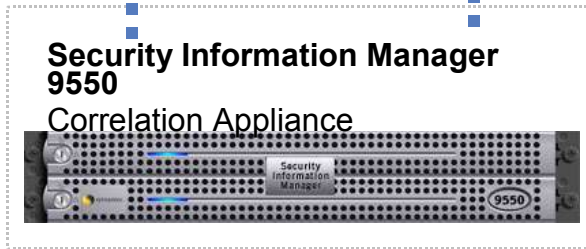
Simplicity

- Veloce installazione & deployment
- Facile uso della GUI
- Pre-configurato embedded datastore & directory
- No DBA richiesto



Global Security Intelligence

- Ultima vulnerabilità e salvaguardia
- Global malicious attack signatures
- Malicious IPs and URLs
- Regole di correlazione



Compliance and Vulnerability Management

- Host and network compliance
- Host and network vulnerability
- Asset discovery/management



Desktop, Gateway and Server Security

- Antivirus, spyware, adware
- Mail and groupware security
- Antispam and content filtering
- Server, HOST IDS, FW



Perimeter and Network Security

- Firewall/VPN
- Routers and switches
- Network IDS/IPS



Deploying Security Solutions

Large Enterprise

Headquarters

Symantec Information Manager 9500 Series

Symantec Network Appliance 7100 Series - 7120, 7160, 7161

Symantec Gateway Security - Model 5660



Symantec Mail Security - 8160

Symantec Mail Security - 8260



Division Office

Symantec Gateway Security - Model 5640



Medium Enterprise

Regional Office

Symantec Mail Security - 8240

Symantec Gateway Security - Model 5620



Small Enterprise

Branch Office Telecommuters



Symantec Gateway Security 1600 Series Models 1620, 1640



Symantec Gateway Security 400 Series - Models 420, 440, 460

Small Business

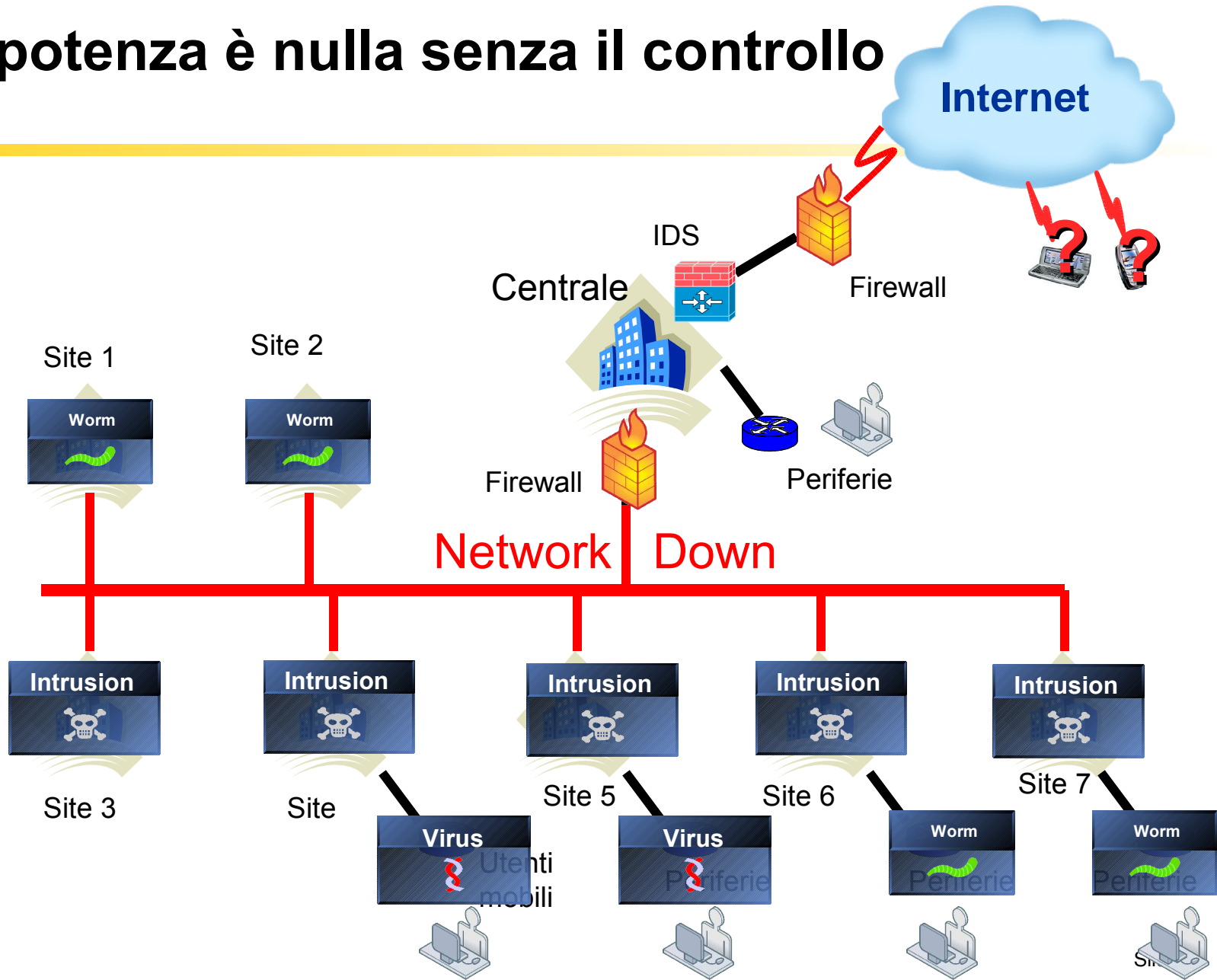
Affordable, Plug-and-Play, Low Maintenance

Powerful, Scalable, Flexible, Cost-effective

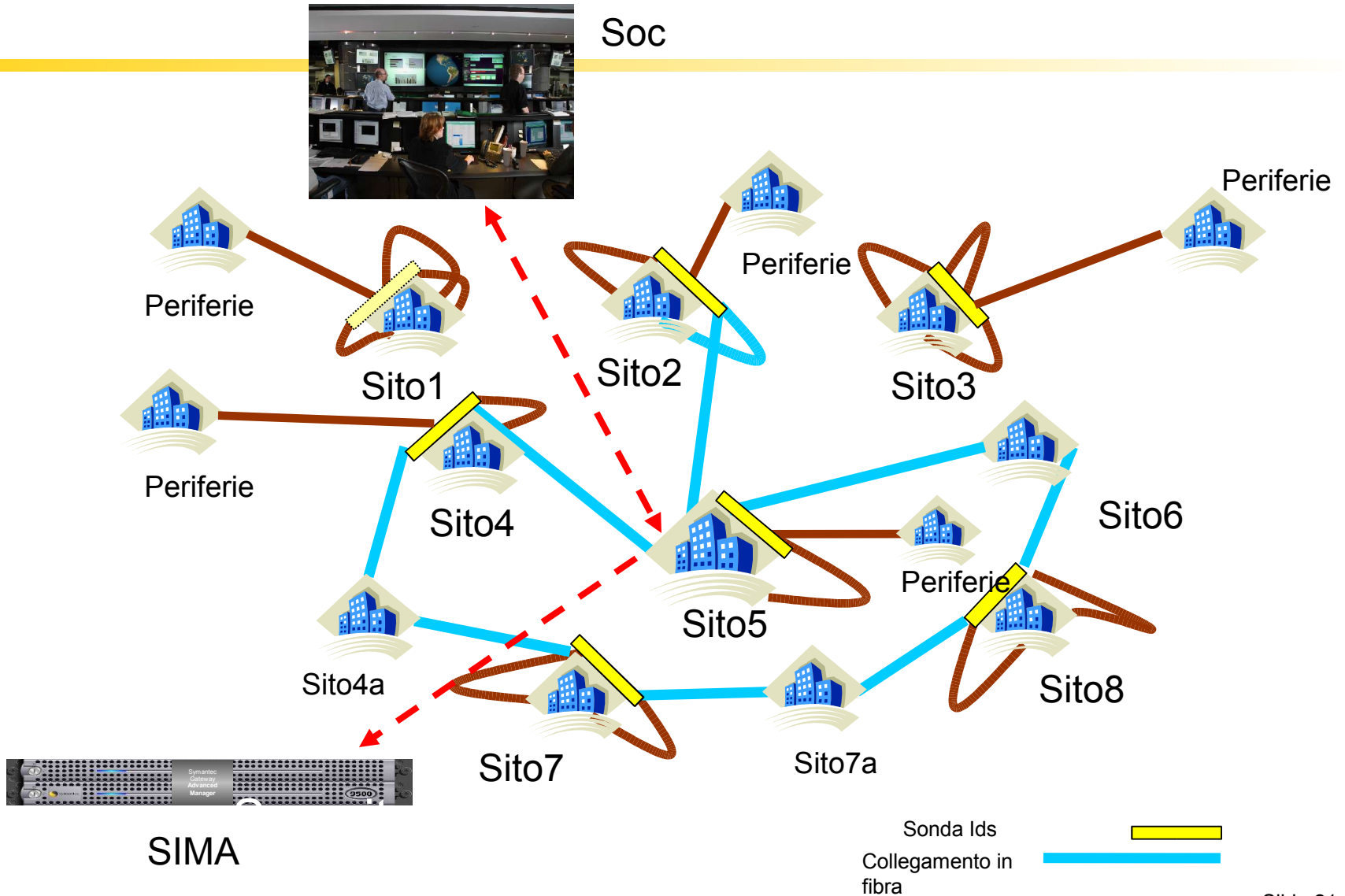
Business Case

- Richiesta di connettività totale
- 100 sedi remote aperte al pubblico
- Centralizzazione dei dati

La potenza è nulla senza il controllo



Incident Handling





DOMANDE ?

Grazie!

Alessandro Gioso