Network Security: un approccio complessivo e progettuale alla sicurezza della rete

InfoSecurity
Milano 13 Febbraio 2004

Giuseppe Borgonovo
Symantec Technical Manager

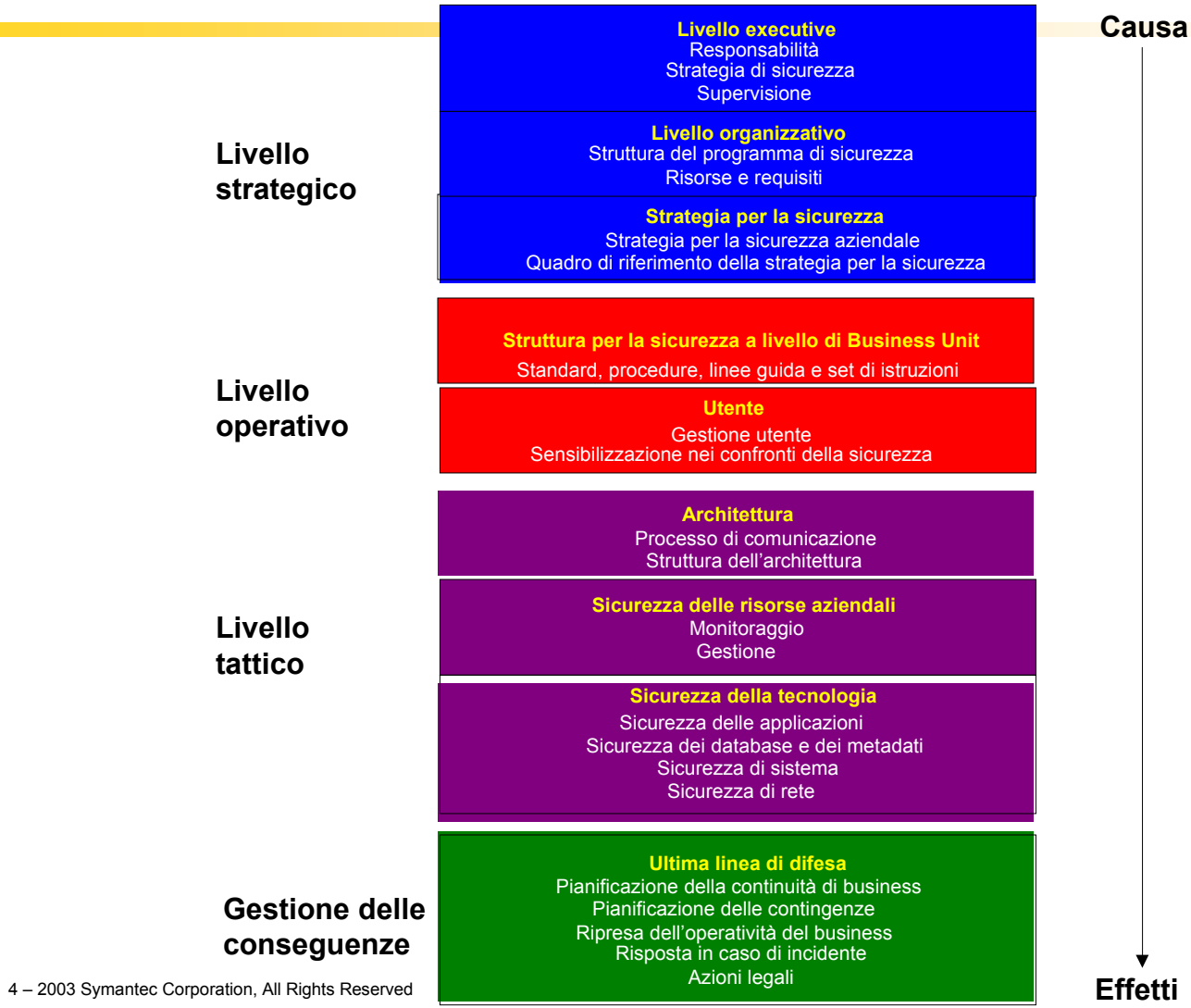
Agenda

- Architettura per la sicurezza
- Metodologia di deployment tecnologico
- I problemi più ricorrenti
- Alcune soluzioni

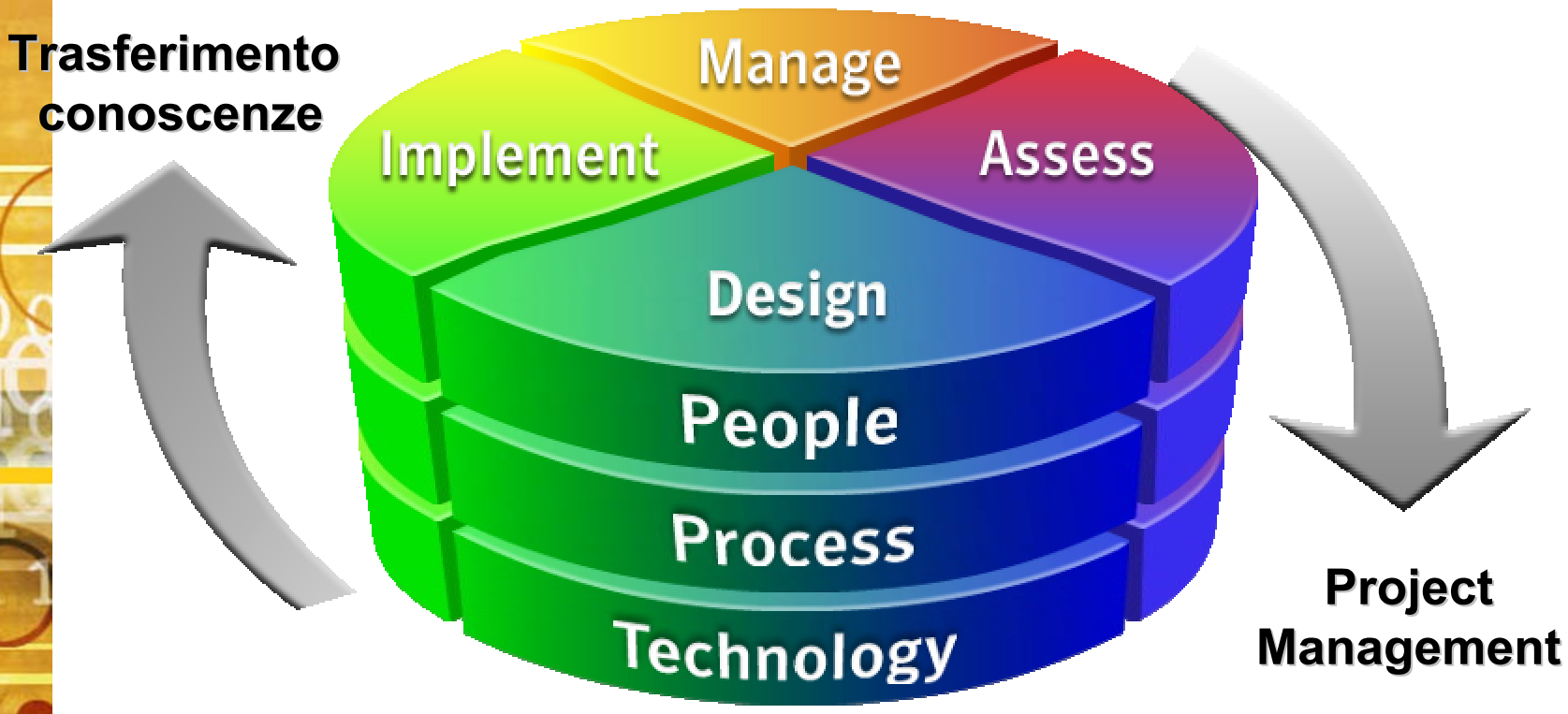
Architettura per la sicurezza

- Sicurezza ≠ semplice tecnologia
- La sicurezza richiede un lavoro di pianificazione ed esecuzione

Sicurezza informatica: modello architetturale



Approccio olistico alle soluzioni per la sicurezza



Persone

- Sensibilizzazione nei confronti della sicurezza
- Le persone giuste – al posto giusto – al momento giusto

Tecnologia

- Noi e loro
- perimetro permeabile
- minacce in evoluzione

- Firewall
- rilevamento intrusioni
- antivirus
- configurazioni
- soluzioni integrate

- Pianificazione
- esecuzione
- messa a punto
- documentazione

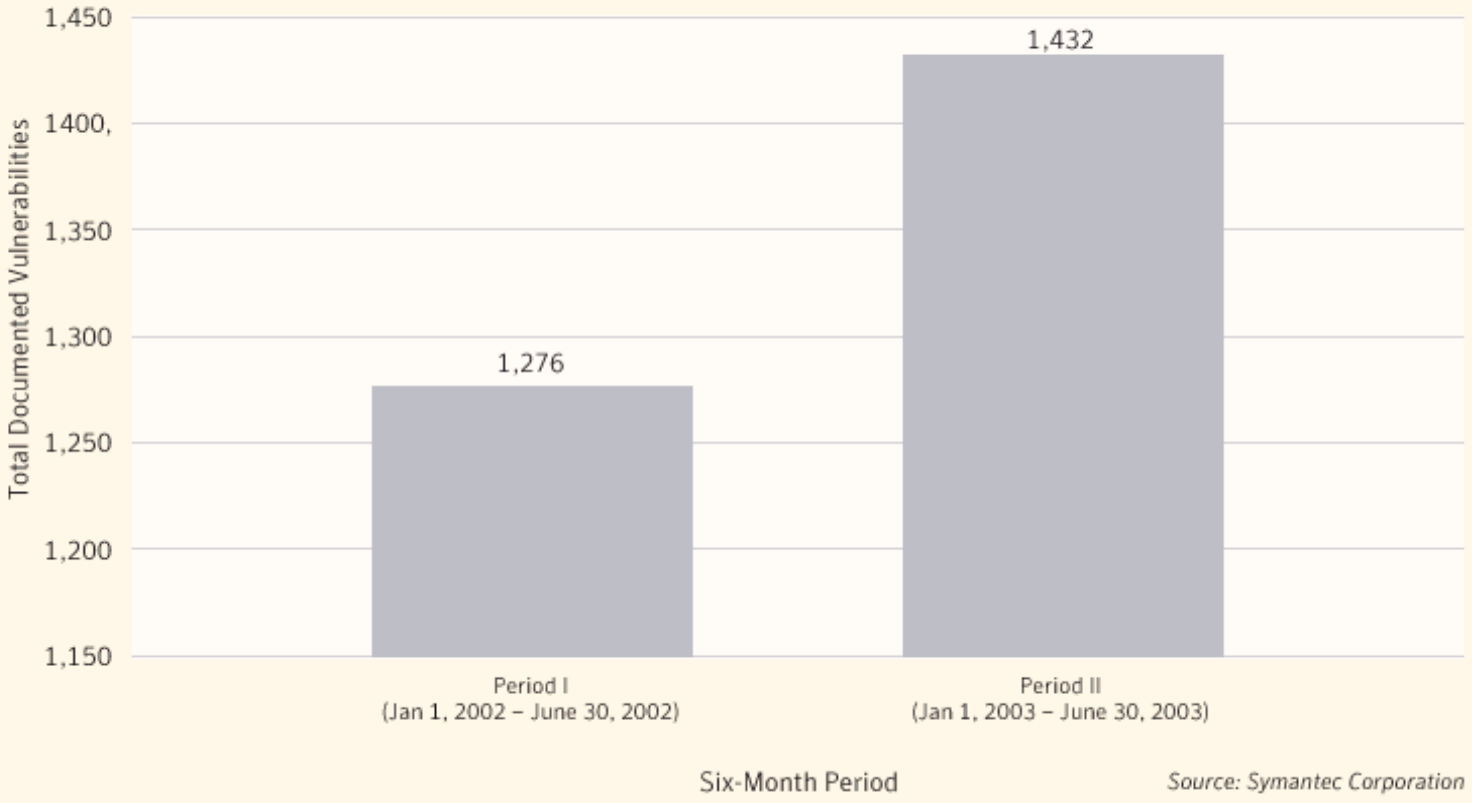
- Gestione della soluzione
- gestione dei risultati

Da cosa ci stiamo proteggendo?

- Utilizzatori non autorizzati
- Utenti autorizzati (fissi e mobili)
- Minacce complesse

Symantec Internet Security Threat Report
1 semestre 2003

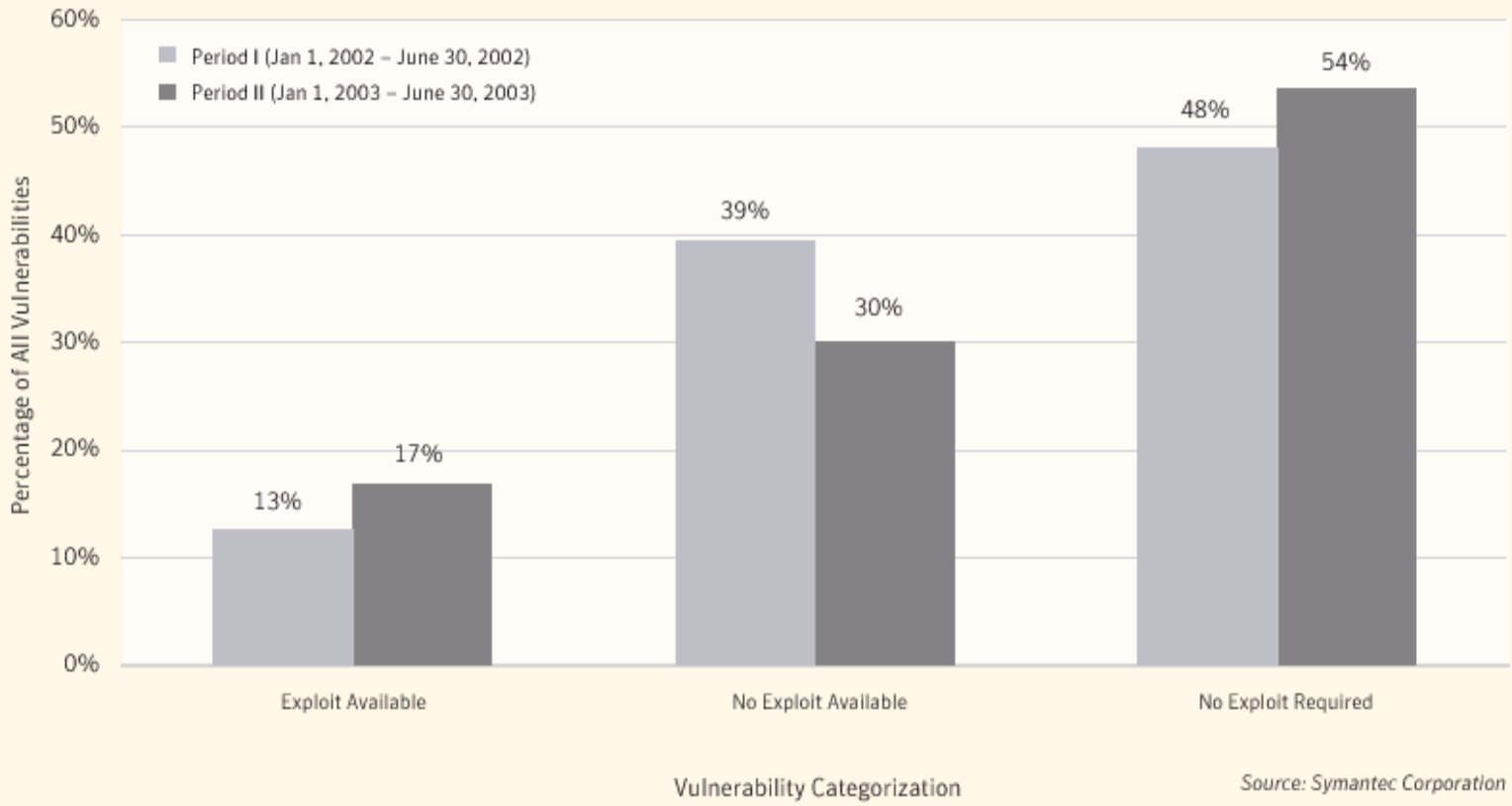
Figure 1: Vulnerability Volume by Six-Month Period
(6 Months Ending June 2002 vs. 6 Months Ending June 2003)



Source: Symantec Corporation

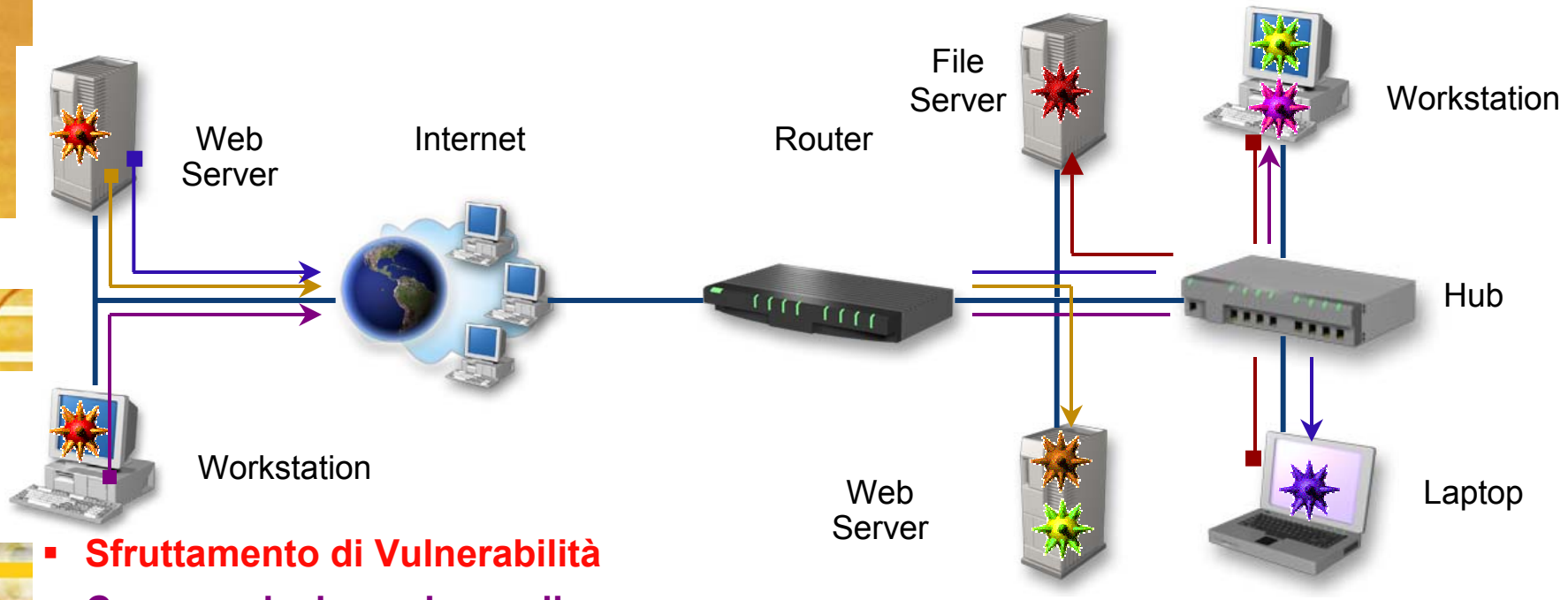
Vulnerabilità \ Exploit

Figure 3: Percent of Vulnerabilities by Ease of Exploitation
(6 Months Ending June 2002 vs. 6 Months Ending June 2003)



Source: Symantec Corporation

Blaster / Blended Threats



- Sfruttamento di Vulnerabilità
- Compromissione via email
- Compromissione di web server
- Contaminazione di files su desktop
- Infezione da web browsing
- Infezione di dischi di rete

Progettazione della soluzione

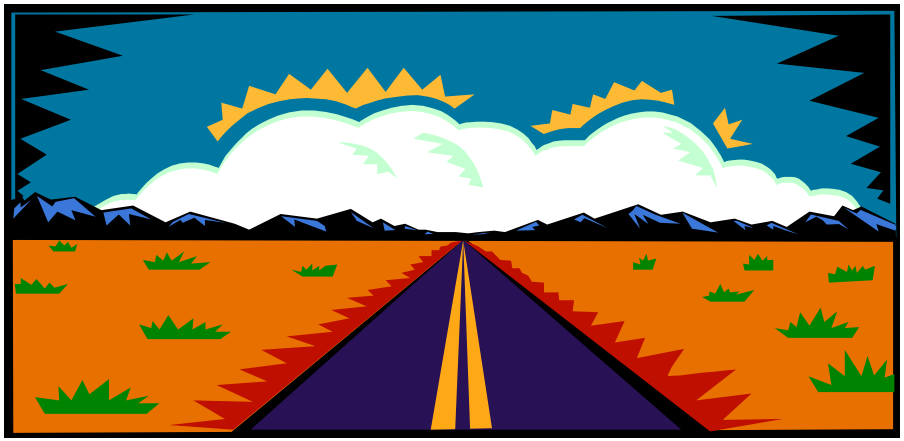
- Protezioni interne
- Protezioni nei punti di transito della rete

Protezione interna

- Antivirus, Personal Firewall
- Analisi delle vulnerabilità
- Gestione della conformità alle procedure
- Sistema di rilevamento delle intrusioni basato su host
- Programma di sensibilizzazione sulla sicurezza

Protezione nei punti di transito della rete

- Filtro dei contenuti
- Firewall a livello di gateway
- Sistema di rilevamento delle intrusioni basato su rete
- Virtual Private Network



Implementazione

- Pianificazione
- Esecuzione
- Messa a punto
- Documentazione

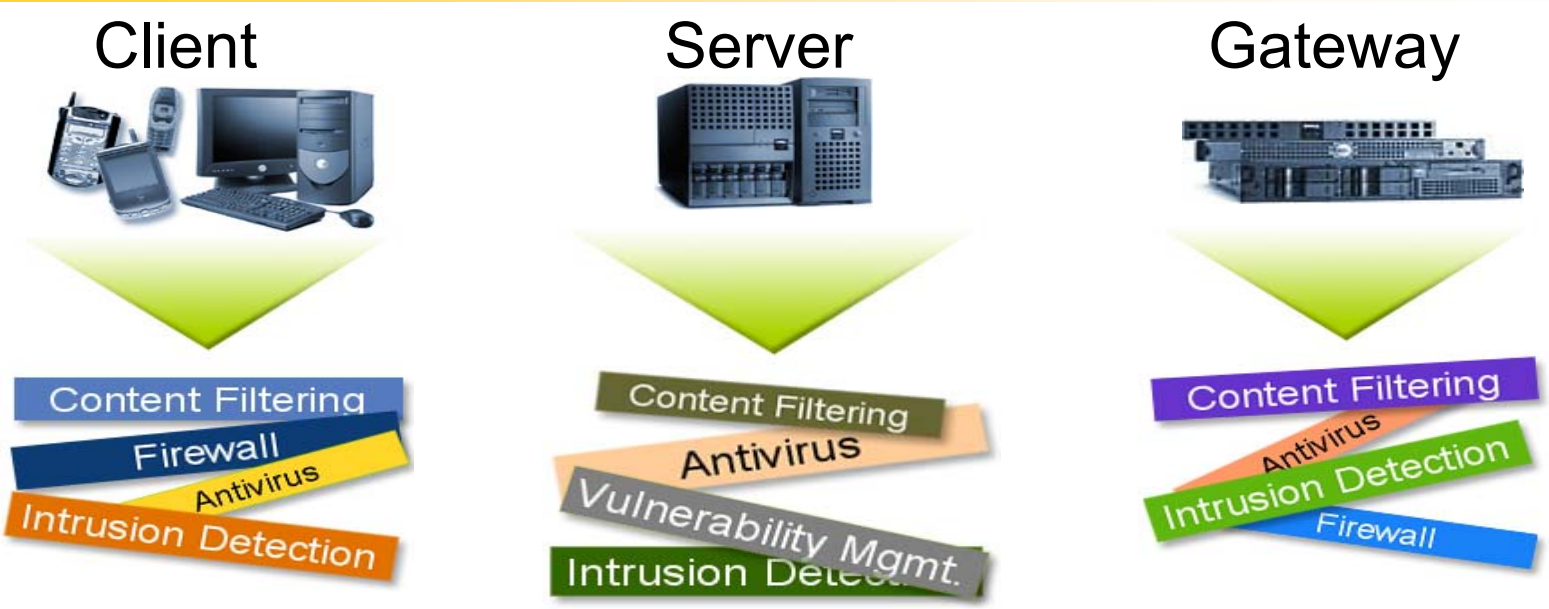
Gestione

- Gestire la soluzione
- Gestire le informazioni prodotte dai sensori di sicurezza
- Risorse dedicate o affidarsi ad un provider di soluzioni di sicurezza gestita
- Opzioni di gestione

Quale approccio seguire

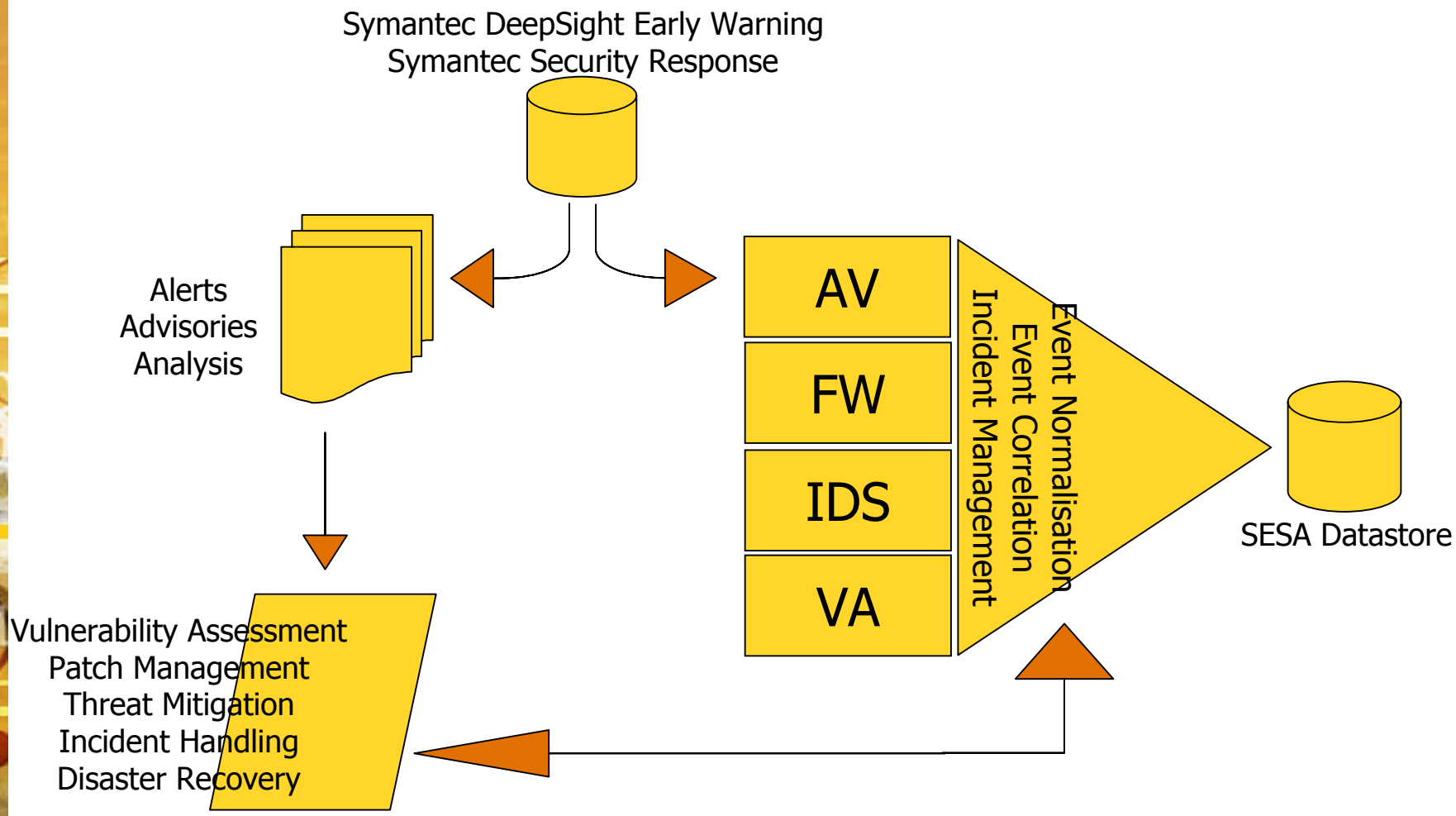
	Benefici	Criticità
In-house	•Controllo completo giorno per giorno •Flessibilità ed adattabilità •Affidabilità interna all'organizzazione •Fortemente integrato con le esigenze di Business Interno	•Tempi lunghi per la predisposizione •Necessità di avere personale altamente formato •Necessità di coprire 24 x 7 •Non rappresenta il core business aziendale
Outsourced		
Managed security service (MSS)	•Tempi brevi per la predisposizione •Servizio fornito 24 x 7 •L'azienda si concentra sul core business	•Perdita di controllo •Fidarsi di provider MSS •Dipendenza dal servizio offerto •Minore integrazione con le esigenze di business interno
Managed security monitoring (MSM)	•Flessibilità ed adattabilità •Persone preparate e affidabili che effettuano analisi •L'azienda si concentra sul core business	•Fidarsi di provider MSM •Dipendenza dal servizio offerto
Co-sourced	•Buon controllo interno sugli elementi gestiti •Crescita professionale del personale interno •Flessibilità ed adattabilità •Persone preparate e affidabili che effettuano analisi	•Perdita di controllo parziale •Fidarsi di provider MSS •Dipendenza parziale dal servizio offerto •Integrazione con le esigenze di business interno

Una tipica strategia per la sicurezza oggi

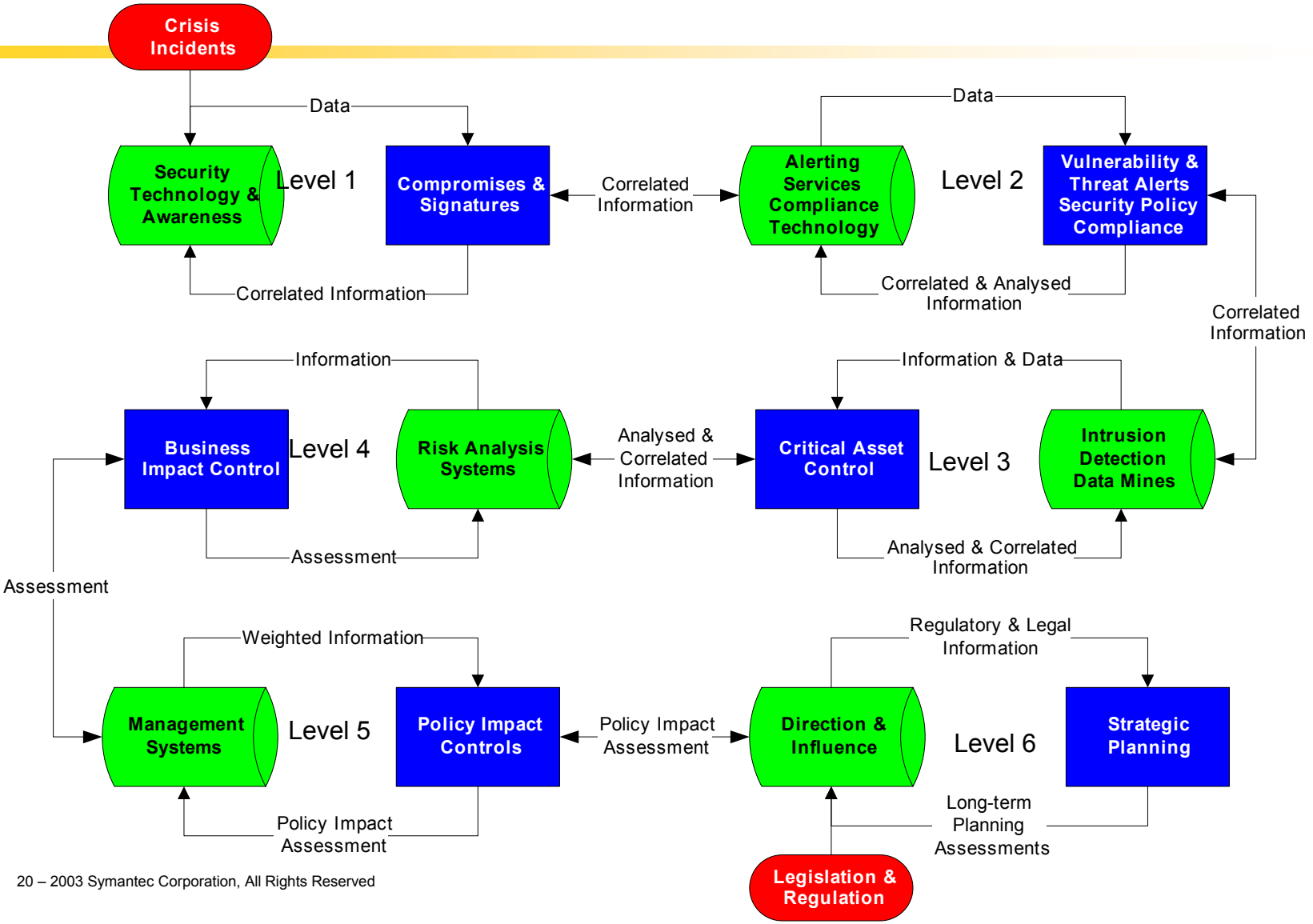


- Frammentazione delle funzionalità di sicurezza
- Non c'è un approccio integrato in grado di proteggere l'intera rete
- Manca una capacità di di gestione unificata della sicurezza
- Disponibilità limitata delle competenze necessarie

Ciclo di protezione dalle minacce - Essere informati e aggiornati in real time



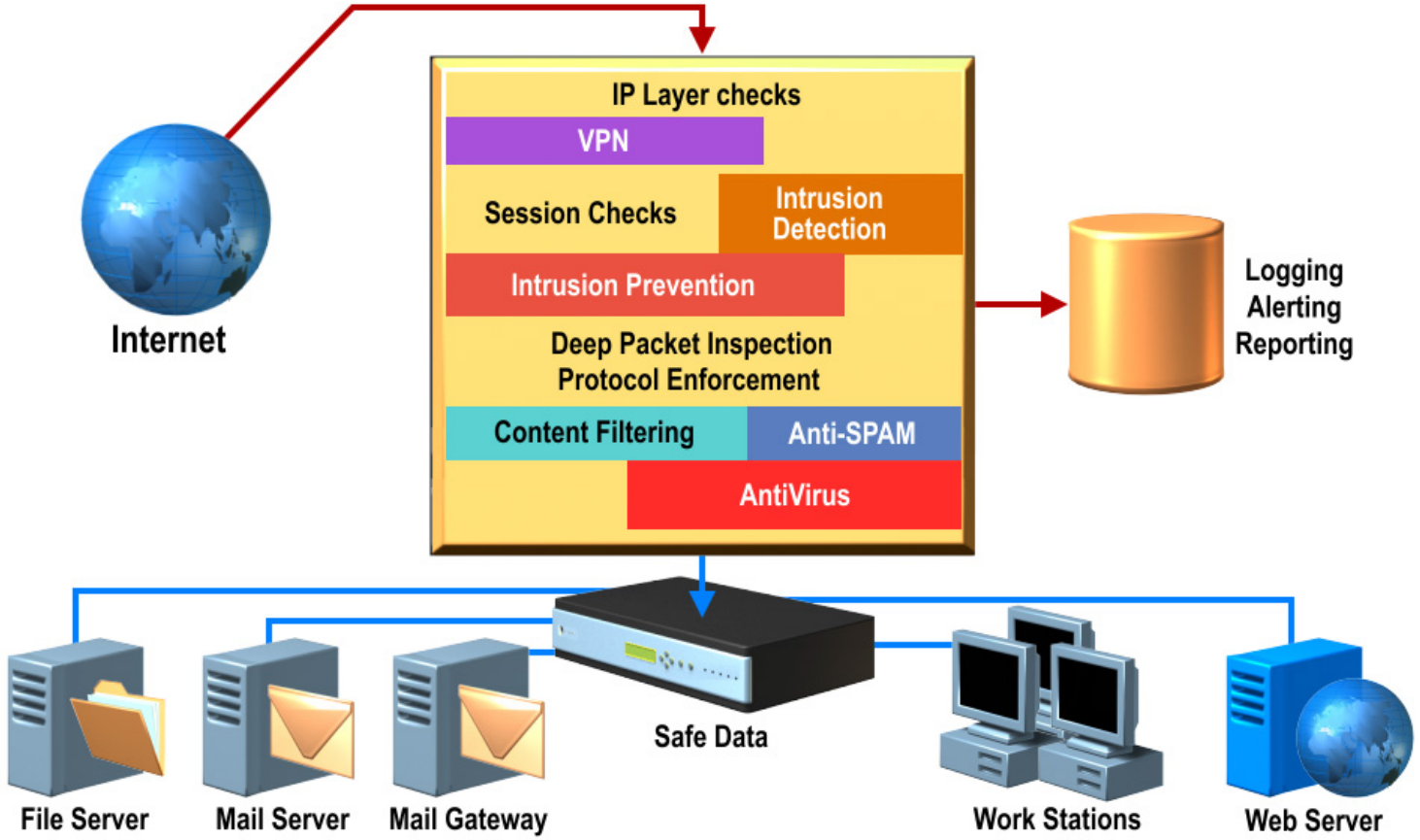
Gestione delle crisi



Symantec DeepSight comunicazioni ai clienti su: W32.Blaster.Worm

- Symantec DeepSight Threat Management System
  - **16/7/03 - Daily Summary Reports Began**
    - Fornite informazioni su vulnerabilità e possibili exploits
  - **25/7/03 - Threat Alert**
    - Informazioni dettagliate su exploit code per la vulnerabilità
  - **7/8/03 - Threat Analysis**
    - Avviso che il worm potrebbe propagarsi rapidamente
  - **11/8/03 - ThreatCon Alert**
    - Aumentato al livello 3 a motivo del worm
  - **11/8/03 - Malicious Code Alert**
    - W32.Blaster.Worm
  - **11/8/03 – Threat Alert**
    - Dettagli su Blaster worm
    - Aggiornamento di tutte le soluzioni AV, FW, IDS, VA
    - Fornite le Snort IDS signatures per la detection

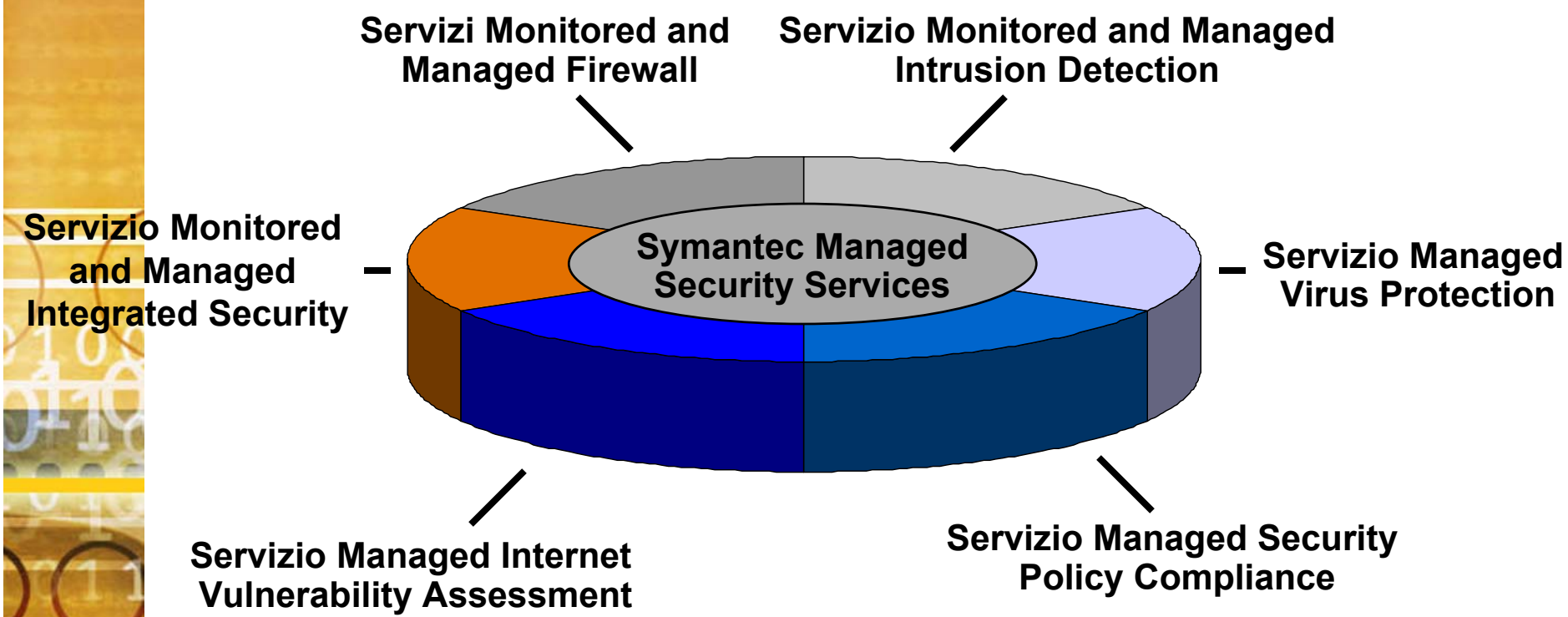
Symantec Gateway Security 5400 series: integrazione di funzioni



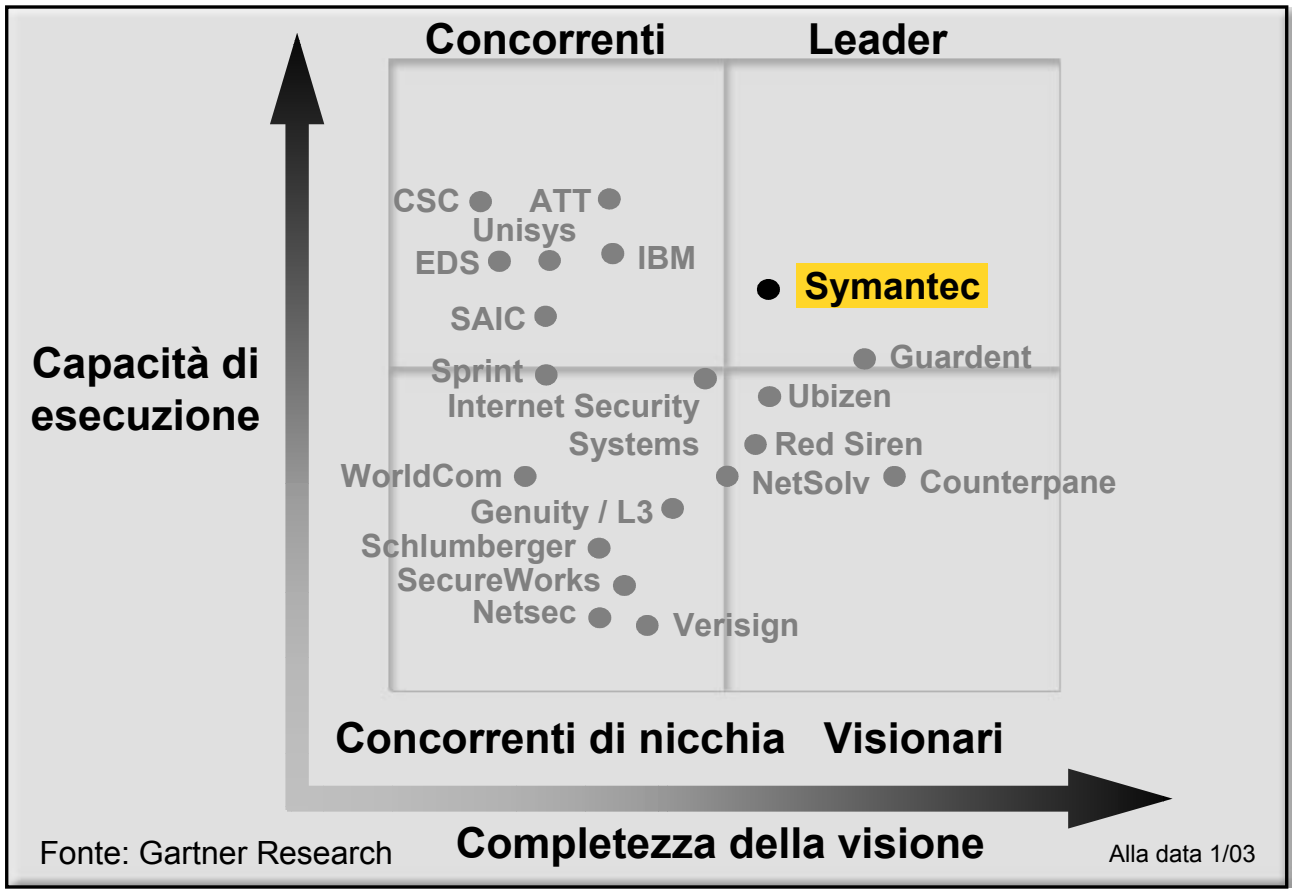
Symantec Clientless VPN Gateway 4400 Series

- Soluzione di accesso per Remote client che fornisce accesso sicuro a risorse aziendali con un Web browser
- Tre differenti modi di operare:
  - Reverse proxy technology supporta nativamente applicazioni Web-enabled ed applicazioni email e file sharing
  - Port forwarding technology fornisce accesso transparent client/server ad applicazioni TCP e UDP
  - Layer 3 VPN tunneling (L3VPN)
    - Illimitato accesso a tutte le applicazioni IP-based
- Policies di accesso per utenti e gruppi multi-livello
- Personalizzazione interfaccia utente (portal pages, automatic tunnel connection, e timeout expiration)
- Integrazione con le comuni infrasfrutture user authentications
  - RSA/SecurID, RADIUS, LDAP, LDAPS, Active Directories, NT Auth, etc.
- Accesso sicuro da ovunque,in ogni orario, a risorse aziendali

Symantec Managed Security Services



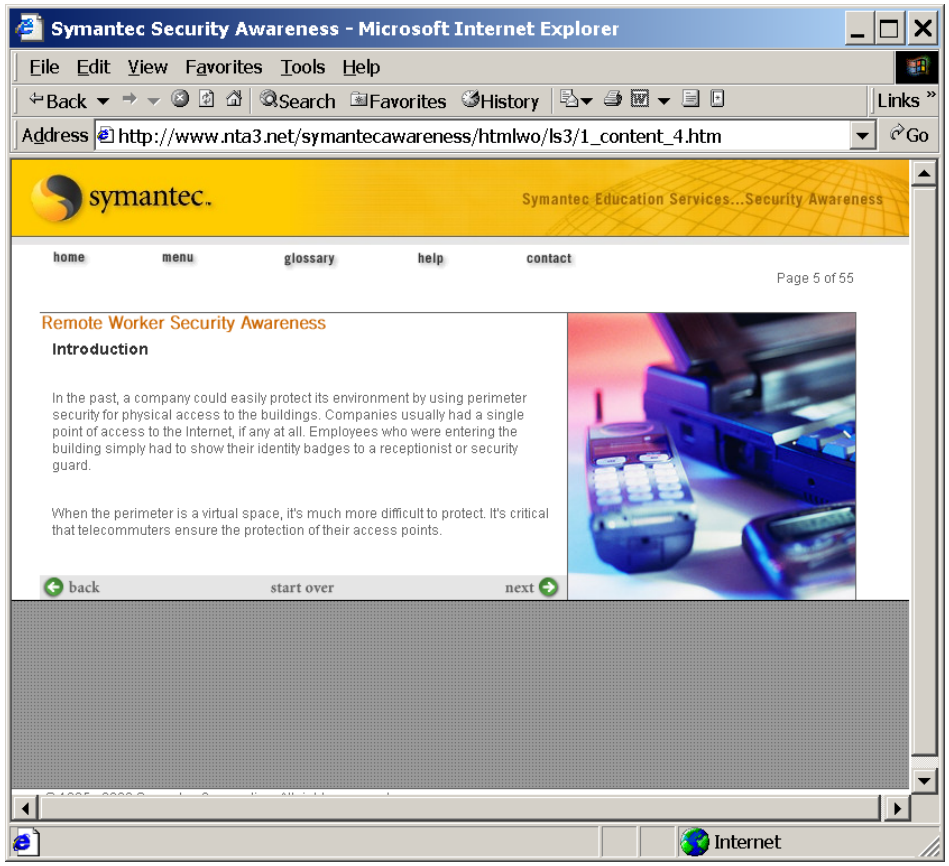
Il punto di vista di Gartner sui MSS



Corporate Security Awareness Program

Soluzione applicativa con l'obiettivo di:

- Sottolineare l'importanza di proteggere le informazioni aziendali
- Formare i dipendenti sui "fondamentali" di sicurezza
- Informare sui comportamenti aziendalmente accettabili
- Valutare il grado di comprensione dei messaggi
- Assicurare un cambiamento di lunga durata nei comportamenti dei dipendenti



Errori frequenti

- Acquistare *prima* e giustificare *poi*
- Acquistare software e non utilizzarlo
- Mancanza di presidio
- Le politiche non vengono messe in atto
- Informazioni disparate e non utilizzate

Domande su cui interrogarsi…

- In che modo sarete messi al corrente quando gli hacker riusciranno a penetrare nelle vostre reti?
- Saprete prevenire, individuare e rispondere a questi attacchi?

Art 4 comma 3 legge 196/2003

"**misure minime**", il complesso delle misure **tecniche, informatiche, organizzative, logistiche e procedurali** di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

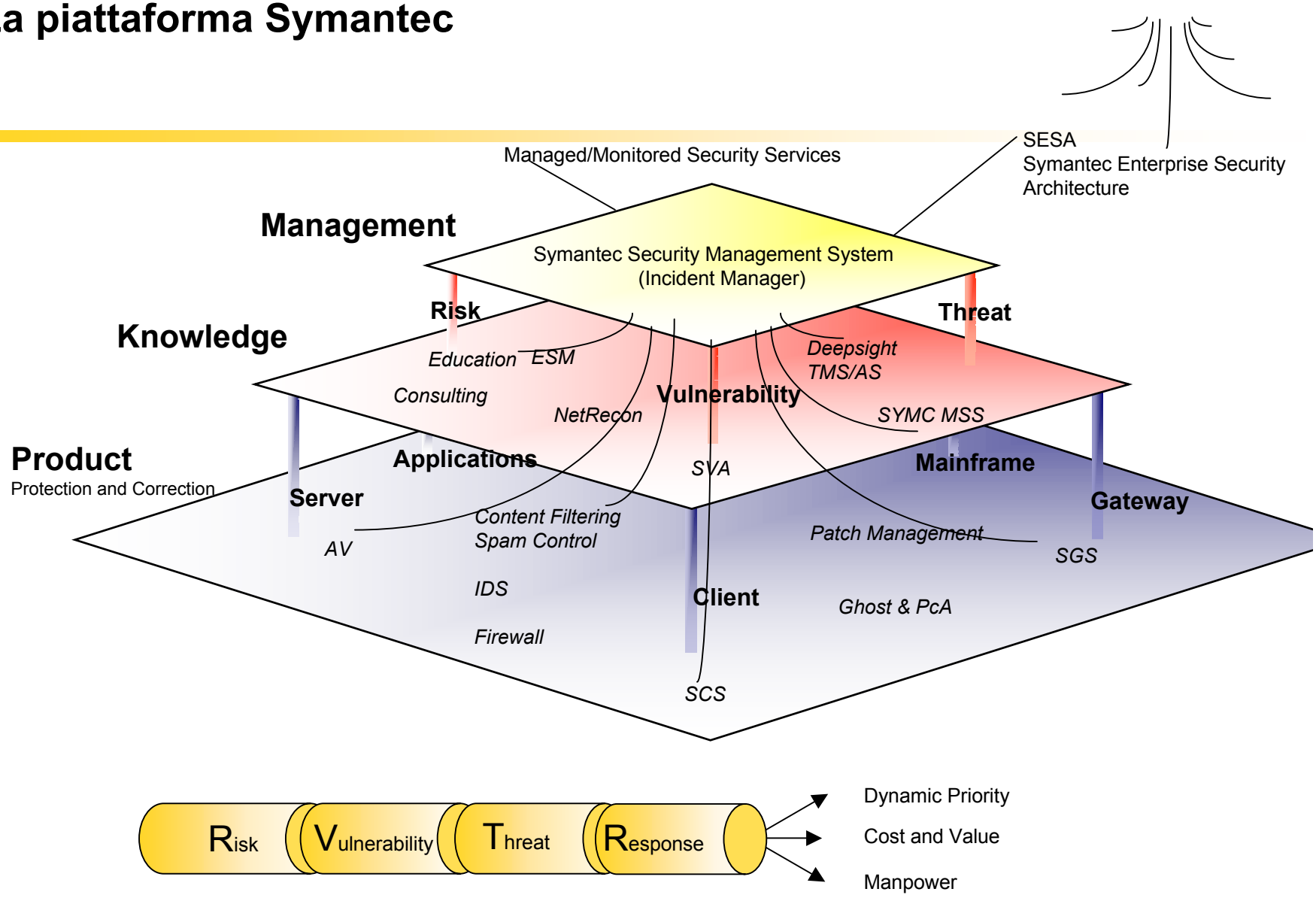
Testo Unico sulla privacy in vigore dal 1-1-2004

Legge 196/2003	Modalità difesa	Strumento
art 31	Difesa perimetrale, controllo accessi, controllo del codice malizioso, copie di dati	Symantec Gateway Security, Soluzioni AV, Manhunt, Symantec HIDS, Ghost, soluzioni PowerQuest di backup
art 34	Difesa perimetrale, controllo accessi, controllo del codice malizioso, copie di dati	Symantec Gateway Security, Soluzioni AV, Manhunt, Symantec HIDS, Ghost, soluzioni PowerQuest di backup
Allegato B punto 16	Difesa da intrusioni, controllo codice malizioso	Symantec Gateway Security, Soluzioni AV, Manhunt, Symantec HIDS
Allegato B punto 17	Controllo e difesa da vulnerabilità	DeepSigth Alert Services, Enterprise Security Manager, Symantec Vulnerability Assessment
Allegato B punto 20	Difesa da accessi abusivi	Symantec Gateway Security, Manhunt, Symantec HIDS

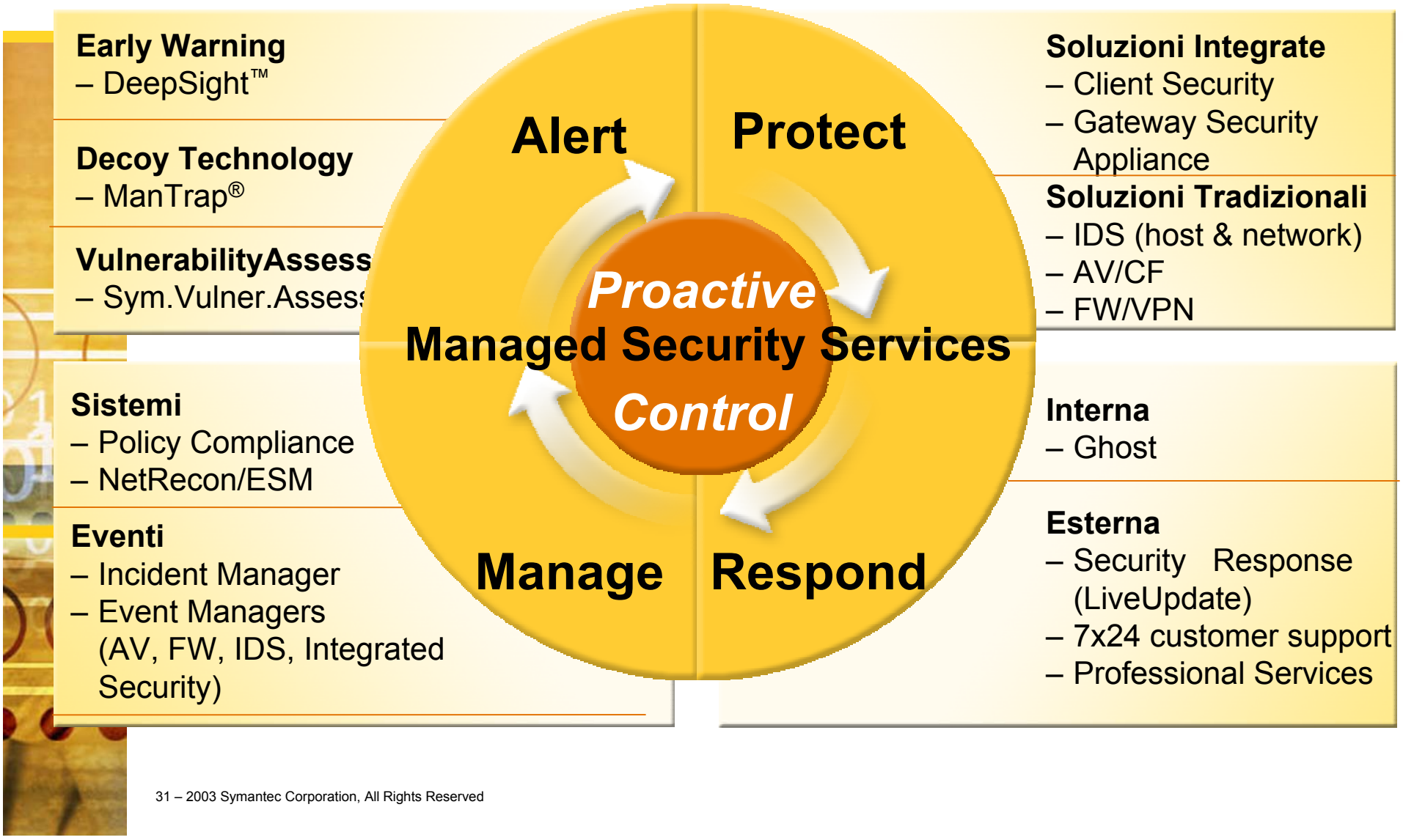
Misure organizzative, procedurali, formazione

Corporate Security Awareness Program

La piattaforma Symantec



Symantec Enterprise Security



Riepilogando

- La soluzione dovrebbe riflettere le politiche / le procedure / gli standard / le linee guida.
- Problemi al vertice si manifesteranno sull'intero modello.
- Una soluzione parziale non è sufficiente

Grazie per l'attenzione!

Giuseppe Borgonovo
giuseppe_borgonovo@symantec.com