



# **CISCO SECURITY MONITORING, ANALYSIS & RESPONSE SYSTEM**

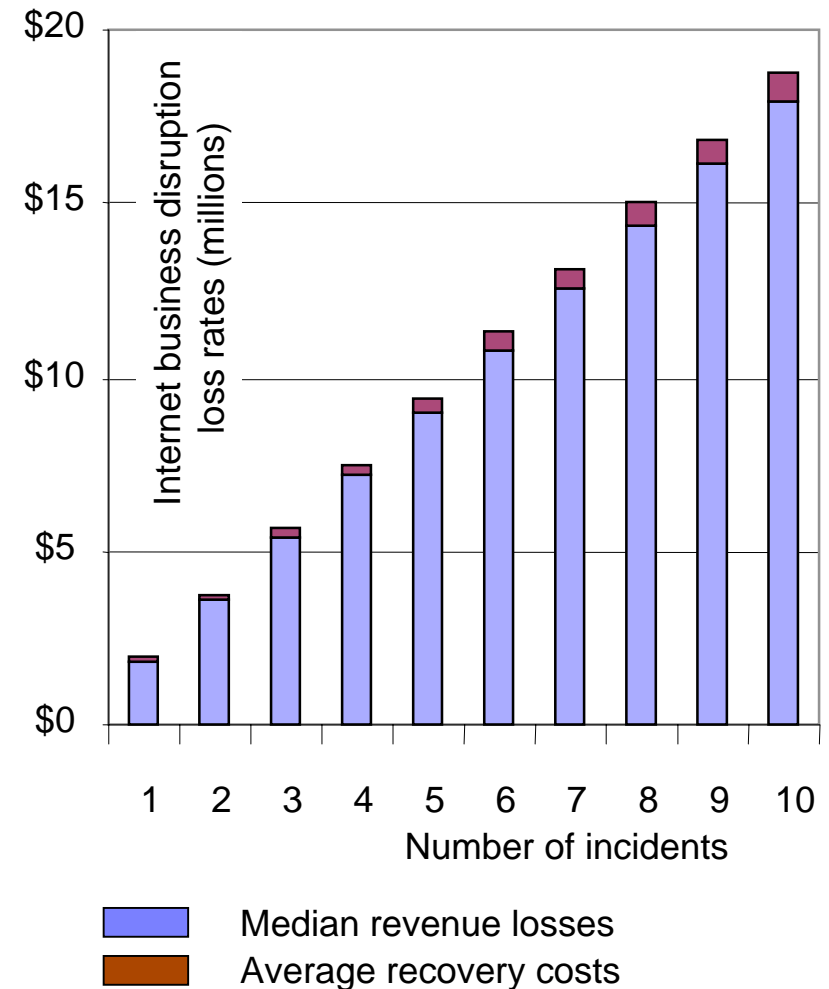
# Mandates and Disruptions

## Mandates:

- Increase customer retention and acquisition
- Build systems around customer/partner access while preserving customer privacy
- Avoid downtime

## Disruptions:

- Direct revenue losses
  - Average \$2,000,000 / incident
  - Median .067% of revenue / incident
- Recovery costs
  - Average = \$74,000 per incident
  - Mean = \$6,000 per incident
- Frequency and duration
  - One incident per year
  - Downtime: 22 hours



\* Aberdeen Group, Automating Information Access Benchmark Research Report, September 2004

# Persistent Attacks and Zero Day Threats

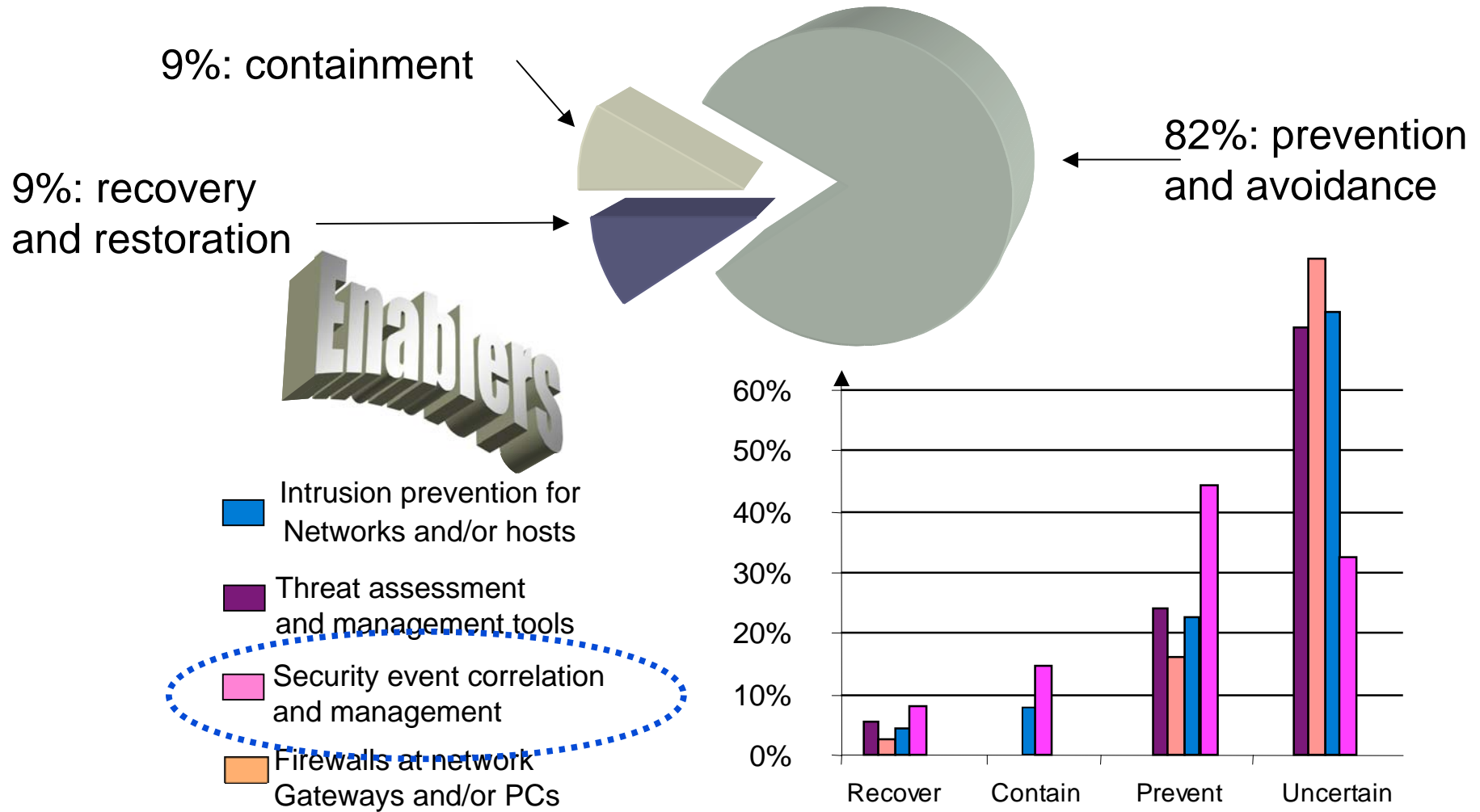
Cisco.com

- Constant Threat of Attacks and Zero-Day Threats
- Companies experience 30+ attacks / week
- Virus and worms attacks increasing at 11% annually
- Slammer infected 75,000 hosts in 11 minutes
- Network Computing estimates the cost per single incident of unknown buffer overflow attack to be \$98,306



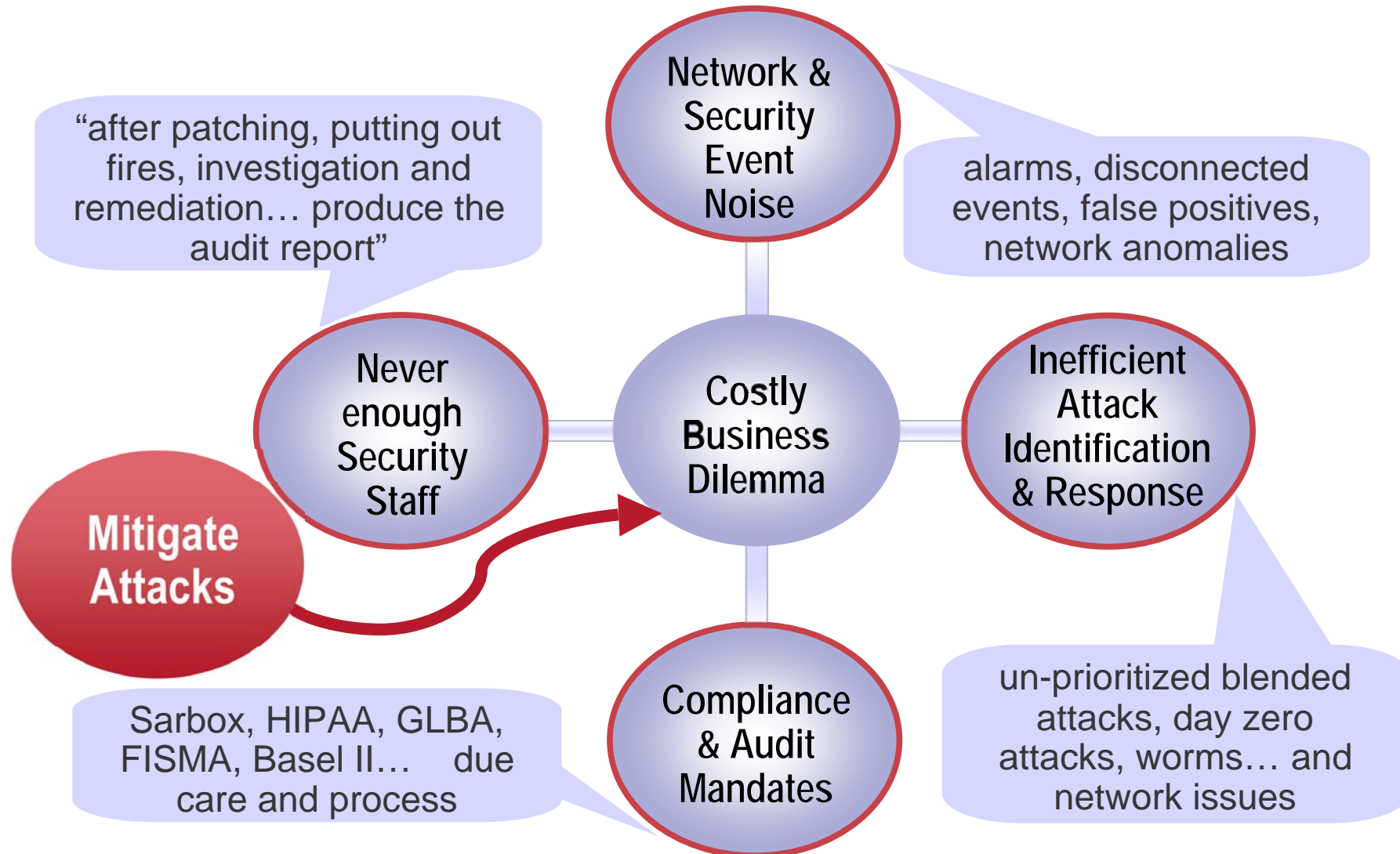
- Variants, scripts, and automated tools essentially yield a persistent attack on open exposures

# Solutions to Overcome Disruptions



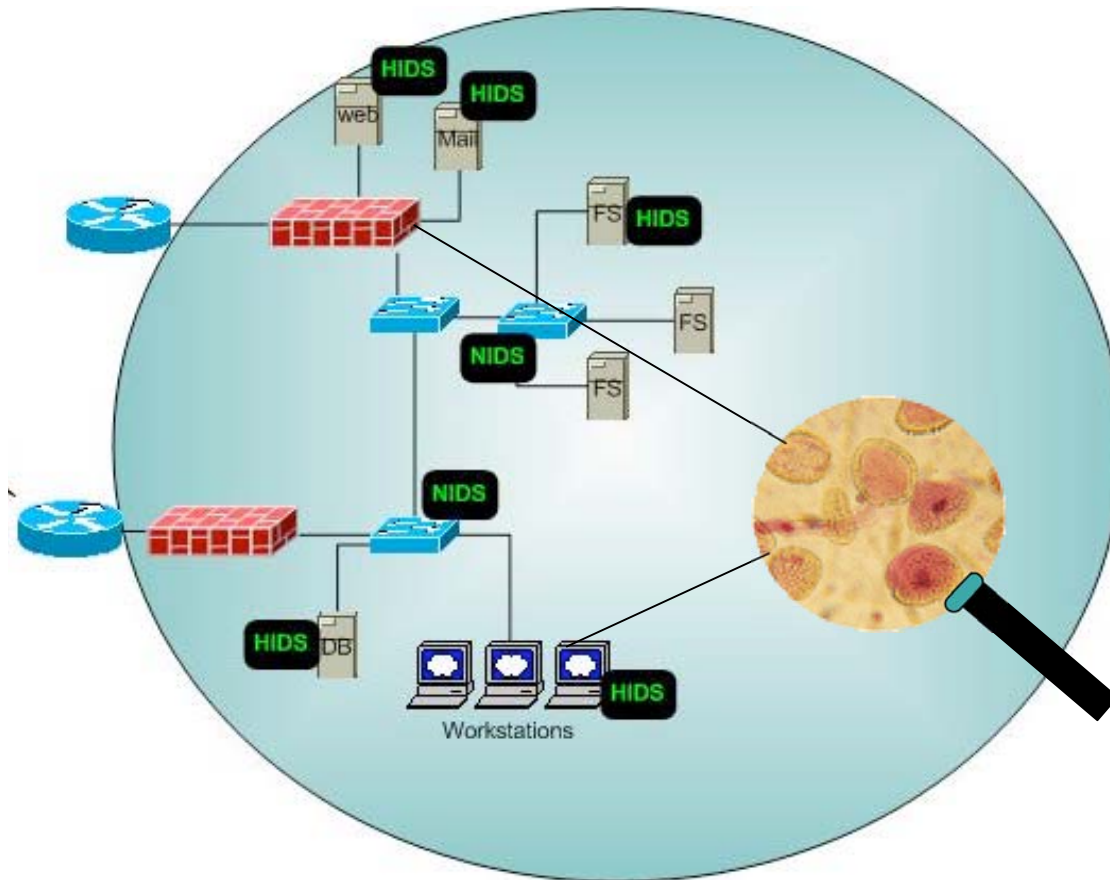
\* Aberdeen Group, Automating Information Access Benchmark Research Report, September 2004

# Security Challenge = Business Problem



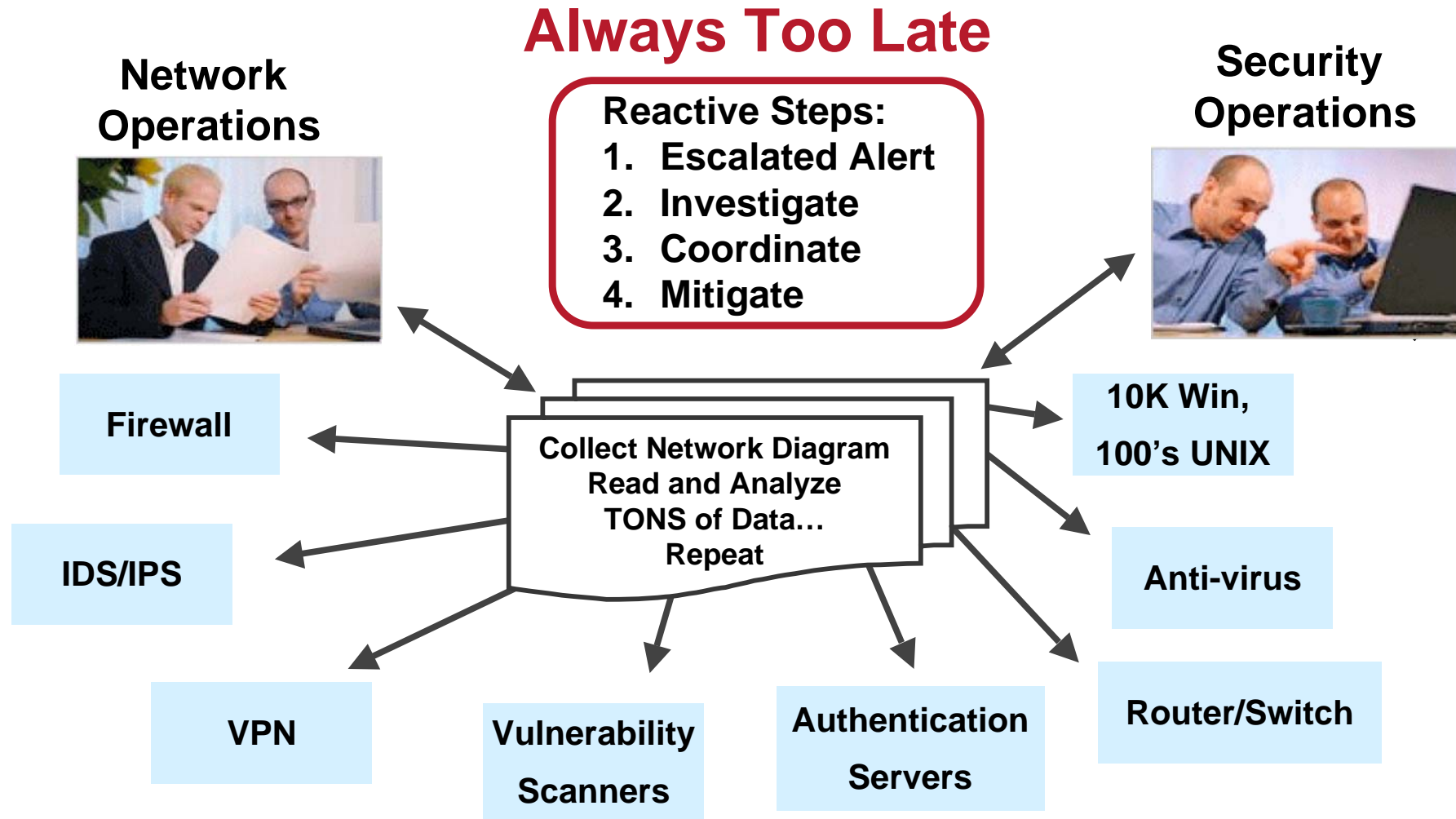
# Components of a Self-Defending Network

Cisco.com



- Defense-in-depth
- Firewalls
- Proxies
- VPN
- Anti-virus
- Network IDS/IPS
- Host IDS/IPS
- Vulnerability Assessment
- Patch Management
- Policy Compliance
- Router
- Switch
- Integrated Management

# Security Operations Response



# Introducing Cisco Security Monitoring, Analysis & Response System (CS-MARS)

Cisco.com

- **CS-MARS transforms raw network and security data into actionable intelligence used to subvert real security incidents, as well as maintain corporate compliance**

- **Network-intelligent correlation**
- **Incident validation**
- **Attack visualization**
- **Automated investigation**
- **Leveraged mitigation**
- **Compliance management**
- **High performance**
- **Low TCO**



# CS-MARS Value Proposition

## Alternative SIM Approaches

## CS-MARS Enterprise Threat Mitigation



Centrally aggregate logs... limited event reduction and correlation

Integrated network intelligence for superior event aggregation, reduction, and correlation



No network intelligence... isolated device events

Events are dynamically NAT resolved, correlated, grouped, and validated



Poor performance; achieved with costly platforms and / or clustering

Full correlation in excess of 10,000 EPS and 300,000 flows / sec



Basic alerts, workflow, and reports... lacks details for timely response

Visually depicts topology, valid incidents; attack path details with layer 2 / 3 leveraged mitigation

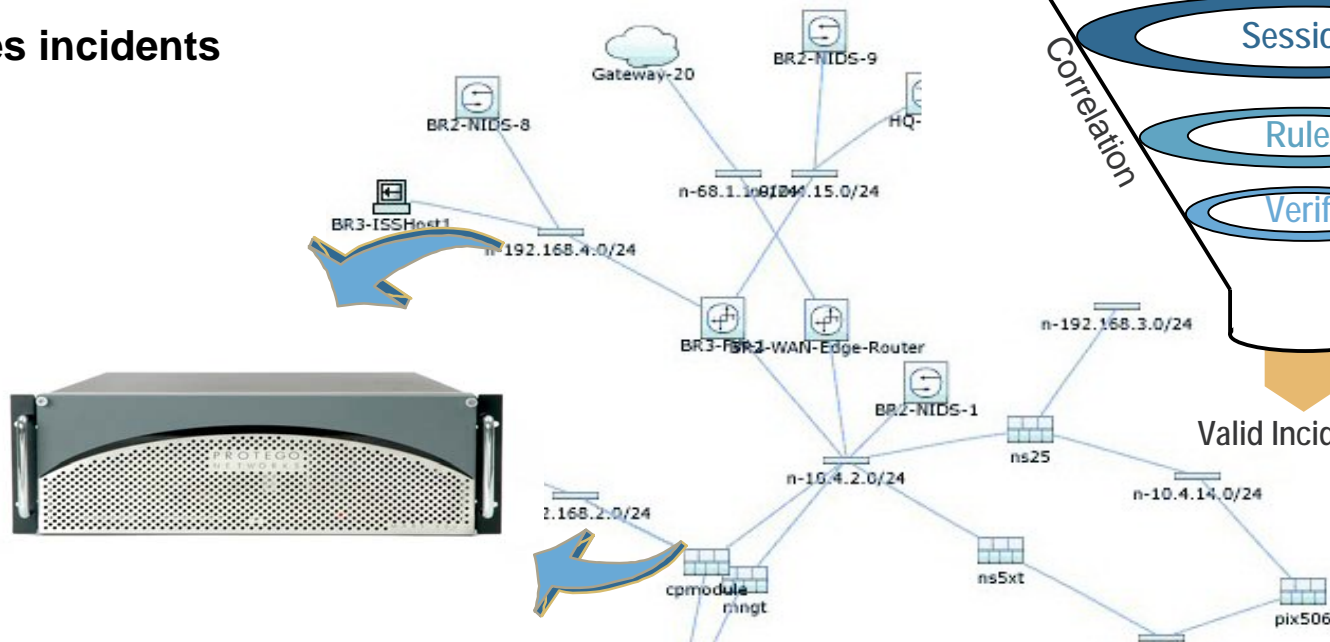
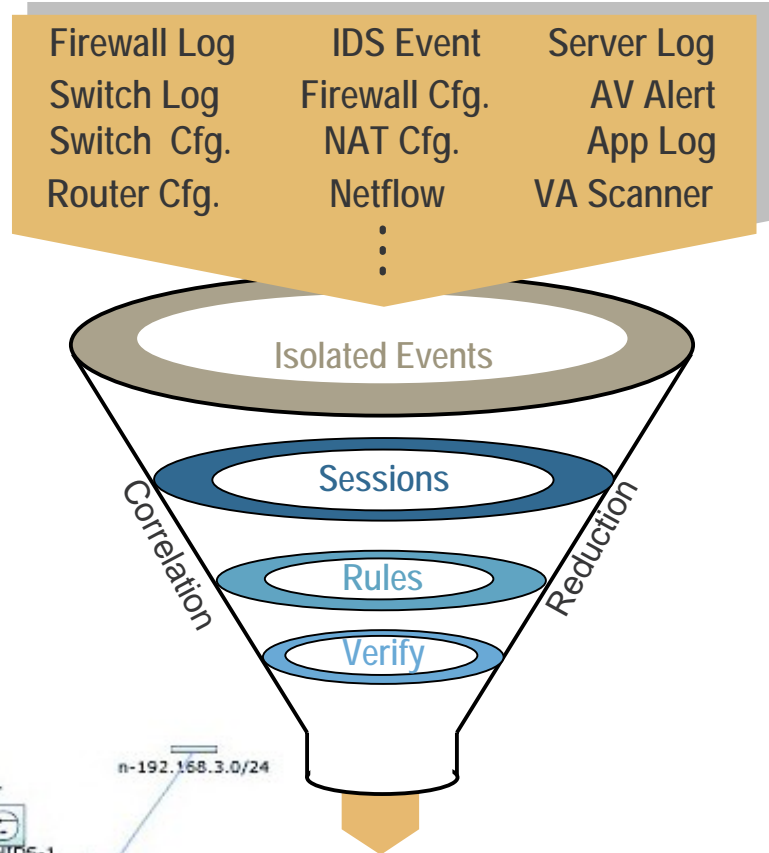


Costly to buy, deploy, maintain


Lowest TCO; immediate results, easy to use and cost-effective deployment

# CS-MARS: “Know the Battlefield”

- **Gain Network Intelligence**  
Topology, traffic flow, device configuration, and enforcement devices
- **ContextCorrelation™**  
Correlates, reduces and categorizes events  
Validates incidents



# CS-MARS: “Command and Control”



SUMMARY | INCIDENTS | QUERY / REPORTS | RULES | MANAGEMENT | ADMIN | HELP

Dashboard | Network Status | My Reports
Nov 3, 2004 2:19:11 PM PST

SUMMARY | PN-MARS Standalone: demo2 v3.1
 

 Login: Gordon, Scott (sgordon) :: [Logout](#) :: [Activate](#)

**Page Refresh Rate**  
 15 minutes ▼

**24 Hour Events**  

Netflow	0
Events	1,315,757
Sessions	515,468
Data Reduction	60%

**24 Hour Incidents**  

High	31	49%
Medium	0	0%
Low	32	50%
<b>Total</b>	<b>63</b>	<b>100%</b>

**All False Positives**  

To be confirmed	14,082	100%
System determined	0	0%
Logged	0	0%
Dropped	0	0%
User confirmed	0	0%
<b>Total</b>	<b>14,082</b>	<b>100%</b>

**To-do List**  
 No Escalated Incidents

**My Reports**  
 No Reports Selected  


[Edit](#)

**Recent Incidents** All Severities ▼

Incident ID	Event Type	Matched Rule	Action	Time	Path
I:45713706	IIS DOT DOT EXECUTE [q], IIS Dot Dot Crash [q], WWW WinNT cmd.exe Exec [q], WWW IIS Unicode Directory traversal [q], IIS CGI Double Decode [q]	Nimda Rule [q]		Nov 3, 2004 1:22:09 PM PST	
I:45713705	Built/teardown/permitted IP connection [q]	Sasser Rule [q]		Nov 3, 2004 1:21:50 PM PST	
I:45713704	Deny packet due to security policy [q]	NetworkConfigError [q]		Nov 3, 2004 12:22:19 PM PST	
I:45713703	Deny packet due to security policy [q]	NetworkConfigError [q]		Nov 3, 2004 12:05:59 PM PST	
I:45713702	IIS DOT DOT EXECUTE [q], IIS Dot Dot Crash [q], WWW WinNT cmd.exe Exec [q], WWW IIS Unicode Directory traversal [q], IIS CGI Double Decode [q]	Nimda Rule [q]		Nov 3, 2004 12:02:41 PM PST	

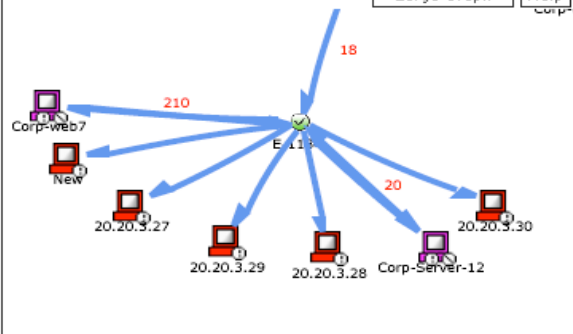
**HotSpot Graph**  

[Full Topo Graph](#) | [Large Graph](#) | [Help](#)



**Attack Diagram**  

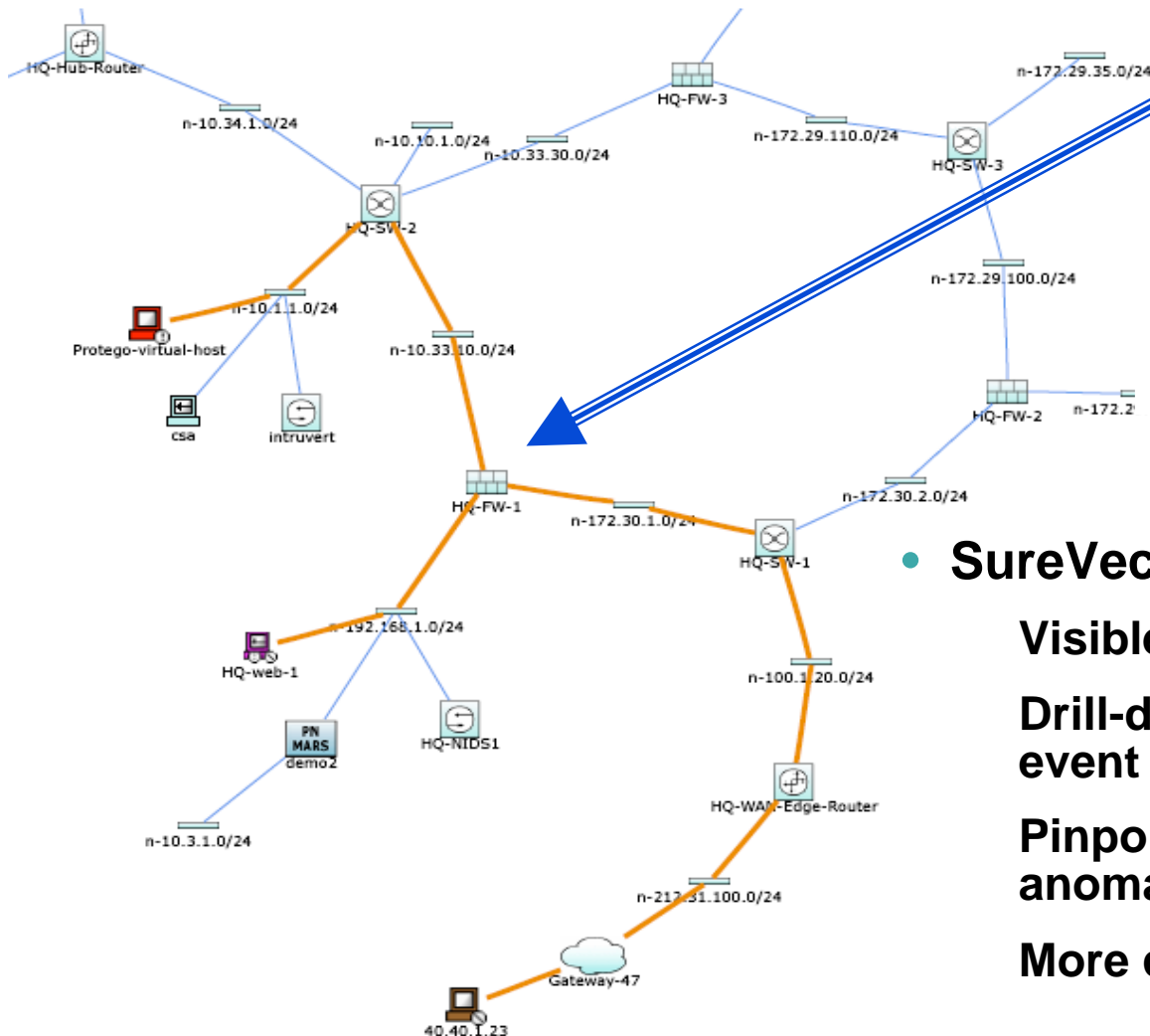
[Large Graph](#) | [Help](#)



© 2005 Cisco Systems, Inc. All rights reserved.

11

# CS-MARS: “Connect the Dots”



1. Host A Port Scans Target X
2. Host A Buffer Overflow Attacks X  
Where X is behind NAT device and  
Where X is Vulnerable to attack
3. Target X executes Password Attacks Target Y located  
downstream from NAT Device

## • SureVector™ Analysis

Visible and accurate attack path

Drill-down, full incident and raw event details

Pinpoint the true sources of anomalous and attack behavior

More complete and accurate story

# CS-MARS “Leveraged Mitigation”

- Use control capabilities within your infrastructure

Layer 2/3 attack path is clearly visible

Mitigation enforcement devices are identified

Exact mitigation command is provided

Enforcement Device: **switch\_server**, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch- IOS 12.2	Protego Networks MARS 1.0 on pivalis		N/A		

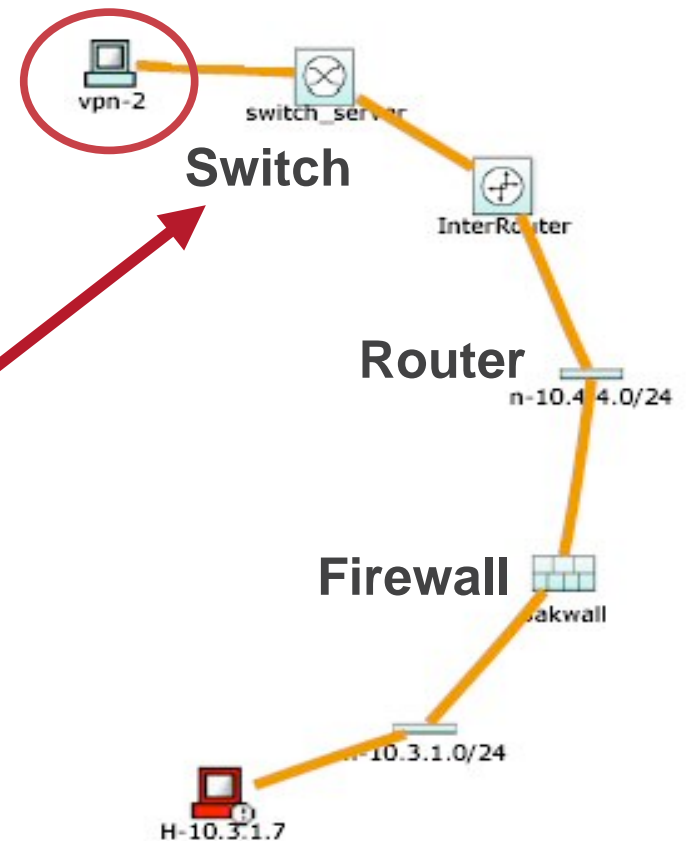
Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
-----------	------------	----------------	----------	-------------	-----------------

Recommended Policy/Command

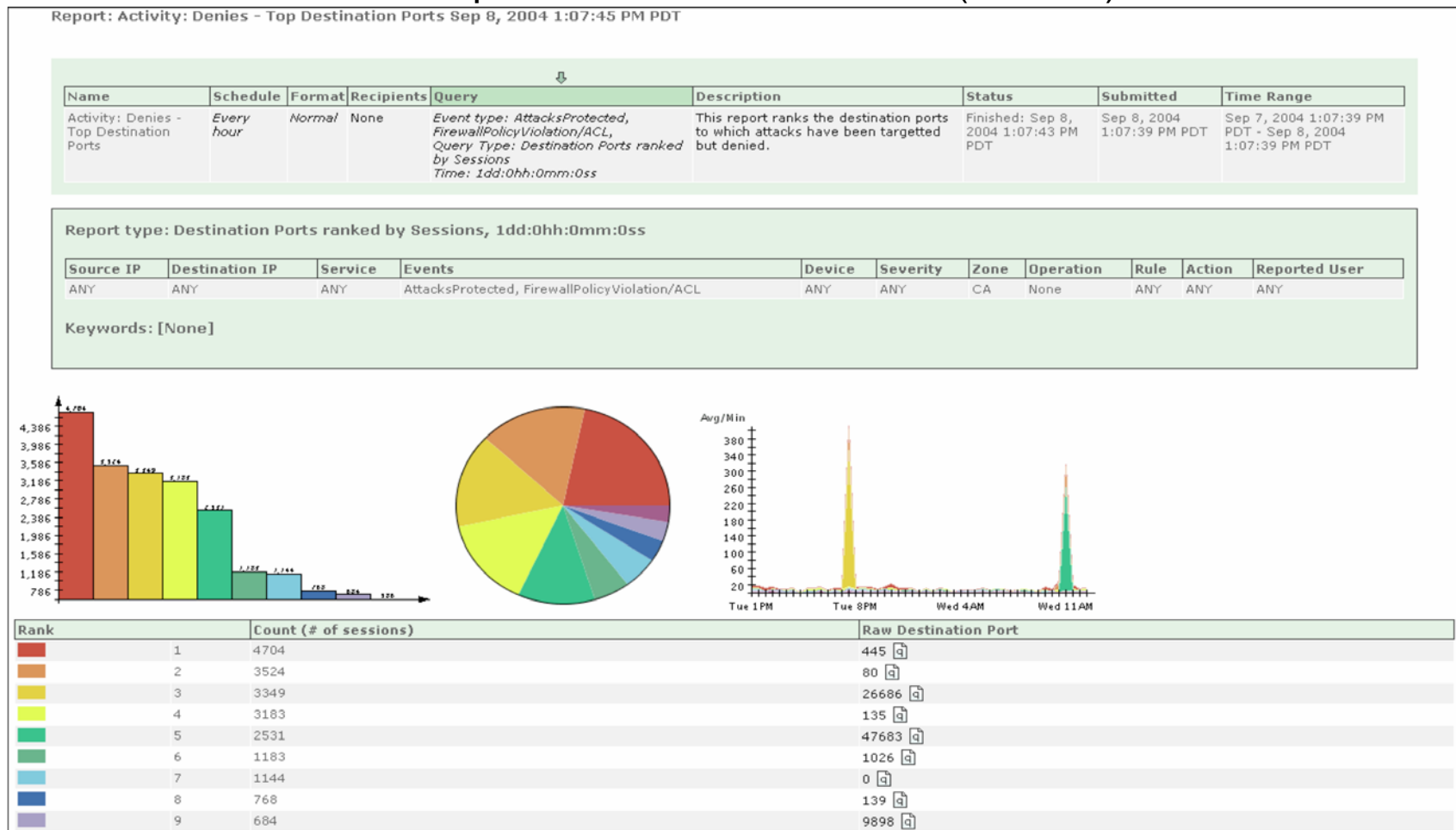
```
configure t
interface FastEthernet0/4
no ip address
shutdown
```

**Push** **Cancel**




# CS-MARS: Compliance Reports

Popular reports with customization and distribution options  
 Queries saved as rules or reports – intuitive framework (no SQL)



# CS-MARS: Correlation and Reduction



Descriptive rule framework and incident details

Significant consolidation

INCIDENTS | PN-MARS Standalone: demo2 v3.2
 
 Login: Gordon, Scott (sgordon) | Logout | Activate

Incident ID: 59235282 Show  
 Session ID: Show

Matched Rule: Successful Recon and Buffer Overflow  
Description: Successful Recon and Buffer Overflow

Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Severity	Counts	Action/Operation	Time-range
1		\$TARGET02	\$TARGET01	ANY	Probe/HostSweep/Non-stealth	ANY	ANY	1	OR	
2		\$TARGET02	\$TARGET01	ANY	Probe/PortSweep/Stealth	ANY	ANY	1	FOLLOWED-BY	
3		\$TARGET02	\$TARGET01	ANY	Penetrate/BufferOverflow/DNS, Penetrate/BufferOverflow/FTP, Penetrate/BufferOverflow/Mail, Penetrate/BufferOverflow/RPC, Penetrate/BufferOverflow/Login, Penetrate/BufferOverflow/Web	ANY	ANY	1	FOLLOWED-BY	
4		\$TARGET01	ANY	ANY	Info/AllSession	ANY	ANY	1		0h:05m

Incident ID: 59235282 Escalate Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Path / Mitigation	Tune
1		ICMP Ping Network Sweep	40.40.1.23	192.168.1.10		Total: 2			
1	S:73993850, I:59235282	ICMP Ping Network Sweep	40.40.1.23	192.168.1.10	ICMP	Nov 22, 2004 7:02:52 AM PST	HQ-SW-1-idsm		False Positive
1	S:73993851, I:59235282	ICMP Ping Network Sweep	40.40.1.23	192.168.1.10	ICMP	Nov 22, 2004 7:02:52 AM PST	HQ-NIDS1		False Positive
3	S:73993900, I:59235282	WWW IIS_ida Indexing Service Overflow	40.40.1.23	192.168.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1, HQ-NIDS1, HQ-SW-1-idsm		False Positive
4		Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10		Total: 3			
4	S:73993871, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive
4	S:73993872, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive
4	S:73993873, I:59235282	Built/teardown/permitted IP connection	192.168.1.10	10.1.1.10	TCP	Nov 22, 2004 7:02:52 AM PST	HQ-FW-1		False Positive

# The CS-MARS Advantage

Cisco.com

- **Superior Functionality, Lowest TCO**
- **Immediate results**
  - Quick install, out-of-box use, web-based HTML console
  - Agentless capture, embedded Oracle®, no dba necessary
  - Supports popular network and security device
- **Optimized performance and scalability**
  - Rapid in-line processing
  - ~over 10,000 EPS with all features active
  - High capacity RAID storage, continuous NFS archive
  - Global controller supports distributed CS-MARS management



# CS-MARS Lineup

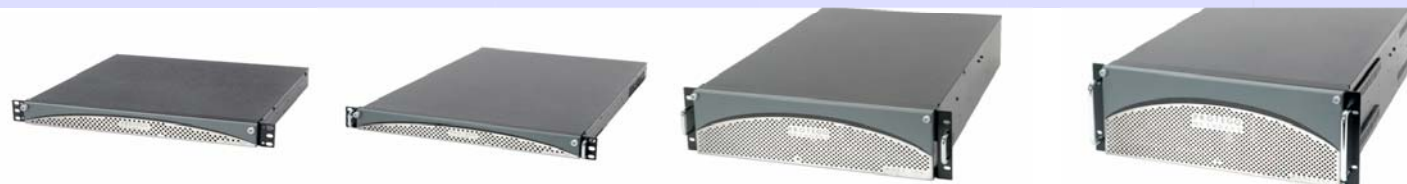
- **Appliance convenience**

**Complete integrated system; no additional hardware, platform, database, or agent software to purchase, install, and maintain**

**No need to determine nodes, admins, agents or other licensing**

**Hardened OS, roles-based admin. and secure communications**

Model	CS-MARS 20	CS-MARS 50	CS-MARS 100e	CS-MARS 100	CS-MARS 200	CS-MARS GC
Events / Sec.	500	1,000	3,000	5,000	10,000	na
Flow / Sec.	10,000	25,000	75,000	150,000	300,000	na
RAID Storage	120GB+	240GB	750GB	750GB	1TB	1TB



+not RAID

# Enterprise Threat Mitigation

Cisco.com

- **Empowers** operators to maintain network availability
- **Leverages** network and security infrastructure
- **Reduces** noise and false alarms for better response
- **Streamlines** investigation, compliance and management
- **Identifies** significant, sophisticated, rapid threats
- **Delivers** return on security investment

## CS-MARS

*Effective. Efficient. Integrated.*



# CISCO SYSTEMS

