Tivoli SecureWay Risk Manager

Venkat Raghavan
Product Management

Tivoli

The Risk of E-business

- e-business risks are similar to bricks and mortar business risks
- Many of the same precautions need to be taken: walls, door locks, insurance, training the staff, a security system, guards … whatever is appropriate to address the expected threats to the business.
- In the new millennium, becoming an e-business is a risk they MUST be willing to take.
- That means ensuring that an centralized and integrated security management strategy is in place for dealing with Denial of Service Attacks and other forms of intrusions

CSI/FBI Survey Highlights

- 90% detected computer breaches in 1999
- 70% reported “serious” breaches like proprietary info theft, fraud, system penetration from outsiders, denial of service, and sabotage
- 74% acknowledged financial losses
- 42% were able and willing to quantify their losses. The total came to $265M.
- The threats continue to come both from inside and outside, with the outsiders now exceeding the insiders for the second year.

2000 survey of 643 computer security practitioners from US corporations, government agencies, financial institutions, medical institutions, and universities,

What are the sources of Risk?

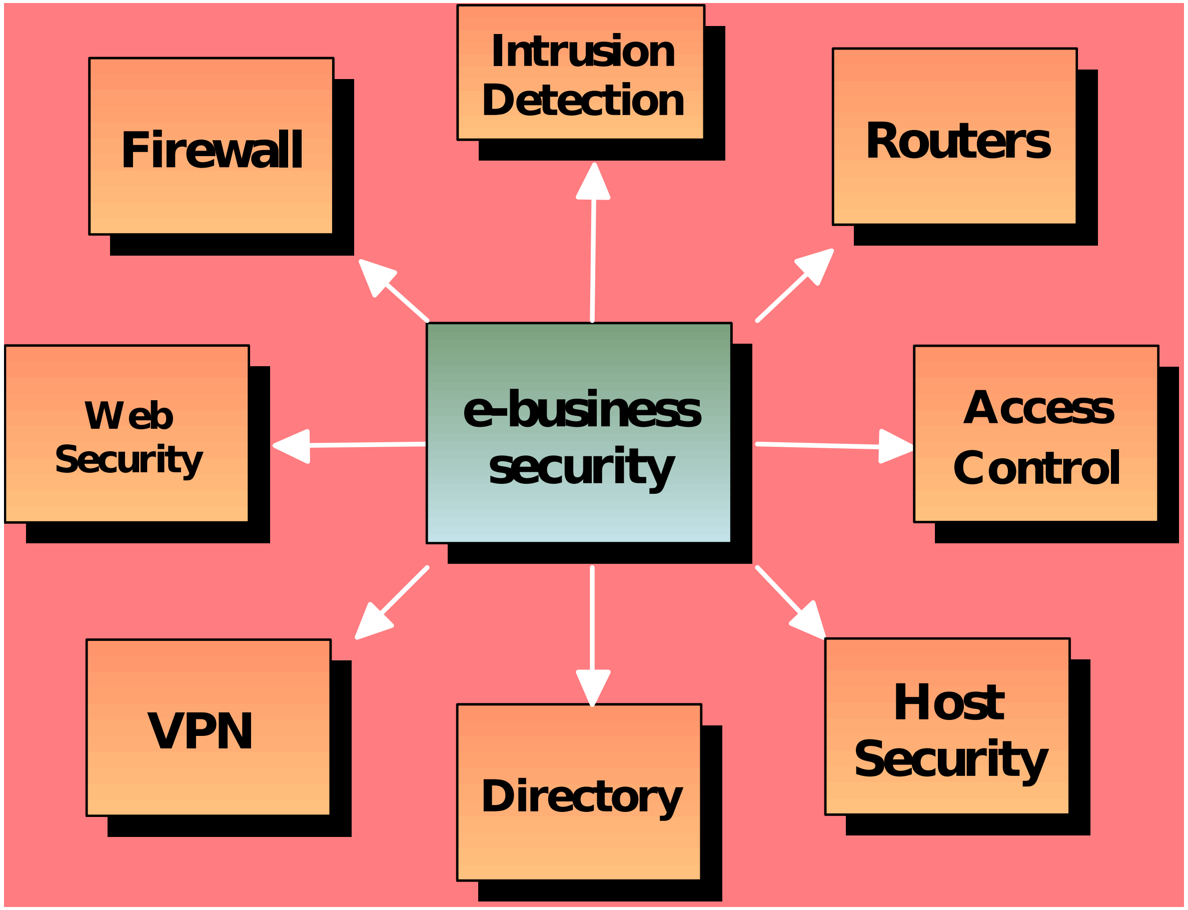
- Today, most of the risks are from hackers
  - motivated by the mere challenge of pushing the security envelope & gaining respect
  - highlighting companies' security weaknesses,
  - winning the respect of their fellow hackers
- A second form of Risk is due to lack of Security expertise
  - A second risk stems from the fact that a high percentage of the individuals involved in building and maintaining web sites and infrastructure, are not well trained in security.

Five Business Issues

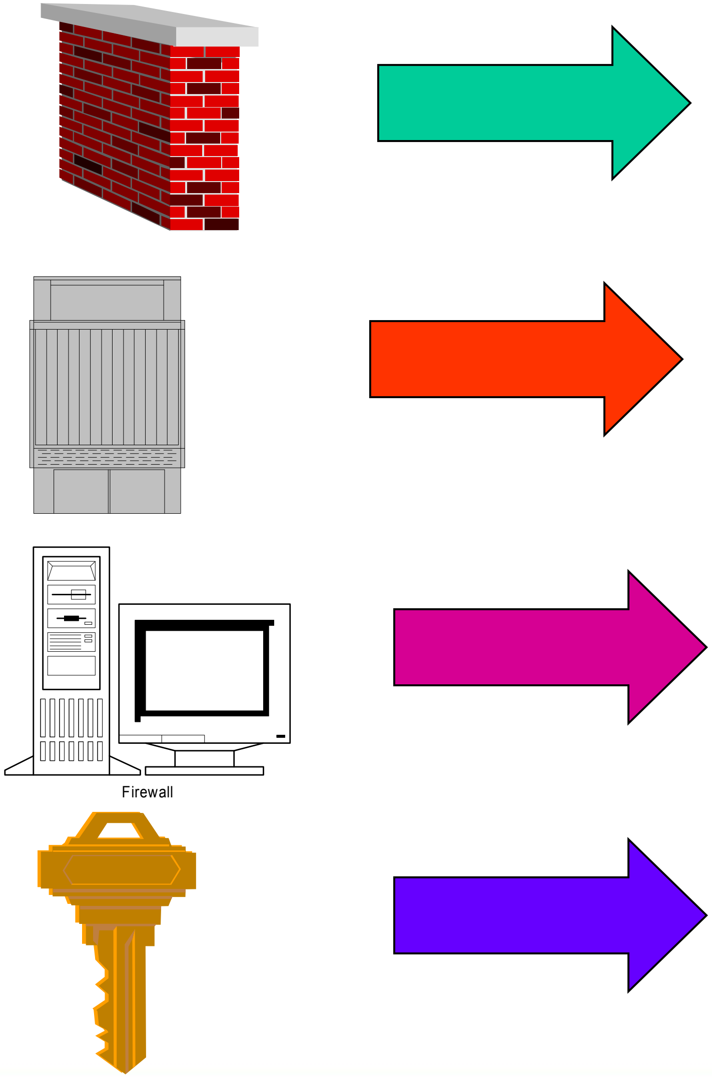
- Necessary Abundance of Point Products
- Technology Increases Complexity
- Scale And Complexity Drive Costs
- Attacks and Intrusions are threats to Business Continuity
- Protect Your Brand Equity

E-business Security Scenario

A collection of Point Products each of which implements specialized security defenses



Point Products



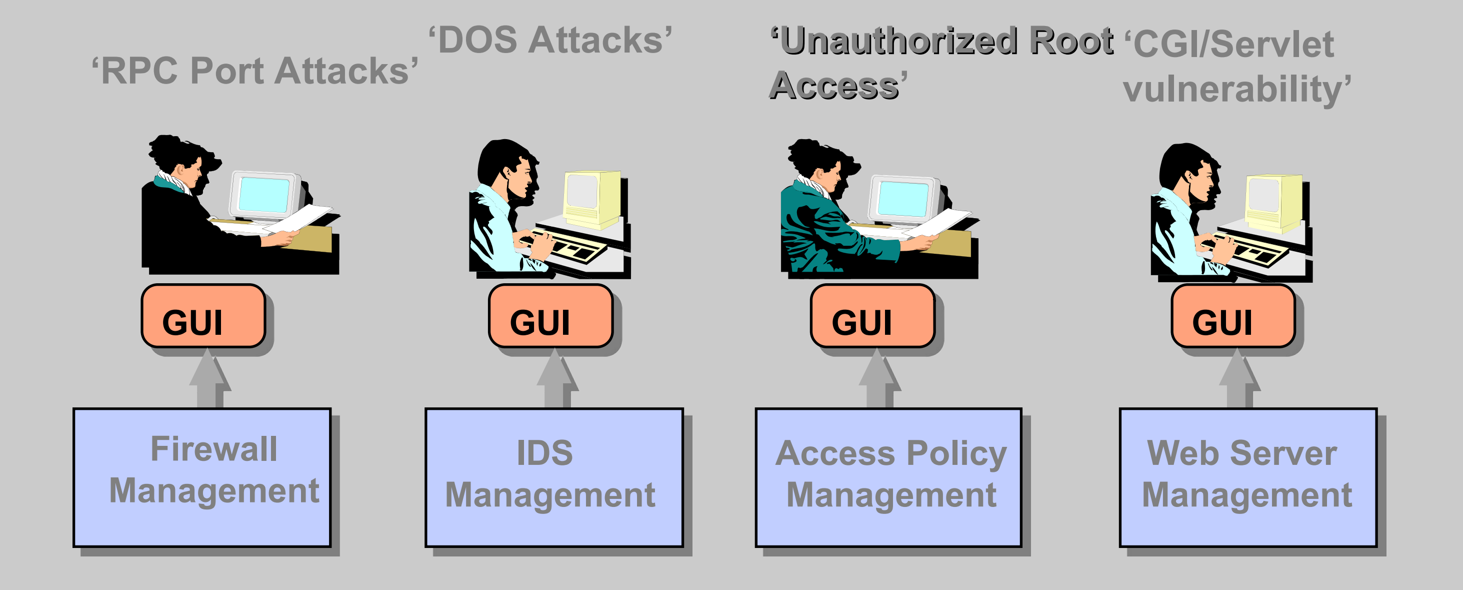
Perimeter Security

Network Intrusion Monitoring

Web Server Intrusion Detection

Authentication & Access Control

Problem: Multiple Point Products, No Integration → *No Control*



- Poor operator productivity because of multiple consoles
- Staff can't zero in on the critical, relevant problems
- Vulnerabilities in point products are often masked
- Hackers can attack the weakest link making the other defenses useless
- Overall security could be compromised by attacking the weakest link

What is Risk Management ?

Security = Risk Management An e-Business has to evaluate its potential for loss, and then decide what steps should be taken to reduce that potential or to limit the loss.

It is not about a specific technology or product - It is about managing the business risks as an overall security management solution

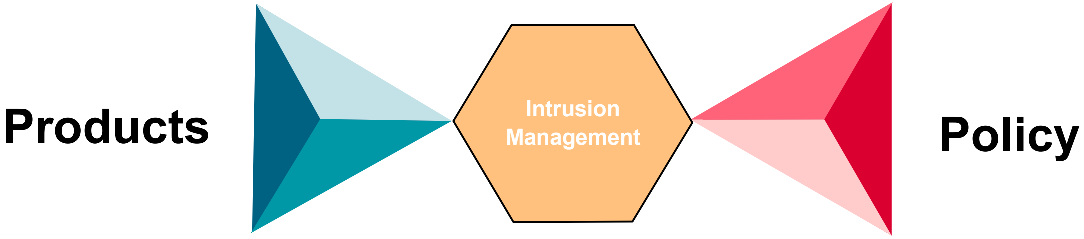
Security risks in the online world carry a much larger downside than those in traditional business: they can quickly erode a brand's value. Just one mistake, a hacked Web site, privacy breach, DOS attack, any incident related to e-business security, and your company shows up on the front page of your favorite magazine or your national newspaper

How we defend against Denial of Service Attacks ?

- Capability to detect and monitor intrusions across multiple sensors
- Capability to detect and remove attack tools
- Capability to detect real attacks from false alarms quickly
- Capability to respond with countermeasures and responses in real-time

These are management problems that require an integrated security management solution

What do you need to manage Risk ?



☑ ◆Technology & Point products

☑ ◆Policies, Practices, Services

☑ ◆Management Tools

An integrated security management strategy requires all three components to deal with Risks

Risk Management

What is Available

☑ **Abundance of Point Products implementing security defenses:** Firewalls, Intrusion Detection, Authenticators, Access Control

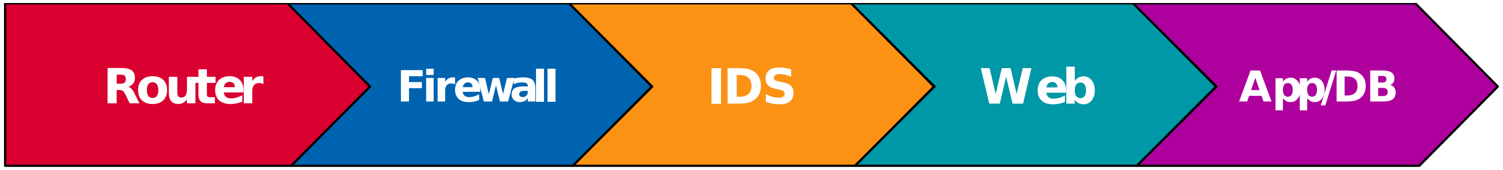
☑ **Policies, Practices & Services**

What is Missing

☒ **Centralized Management of Threats & Intrusions across different Point Products**

Why is Centralized Risk Management Important

- Security is a Link. Each point product implements only a small subset of the security policy
- What the Screening Router/Firewall cannot block
  - The IDS should detect
    - What the IDS doesn't see the Web security mechanism must see
      - What the Web doesn't see the App/database must see



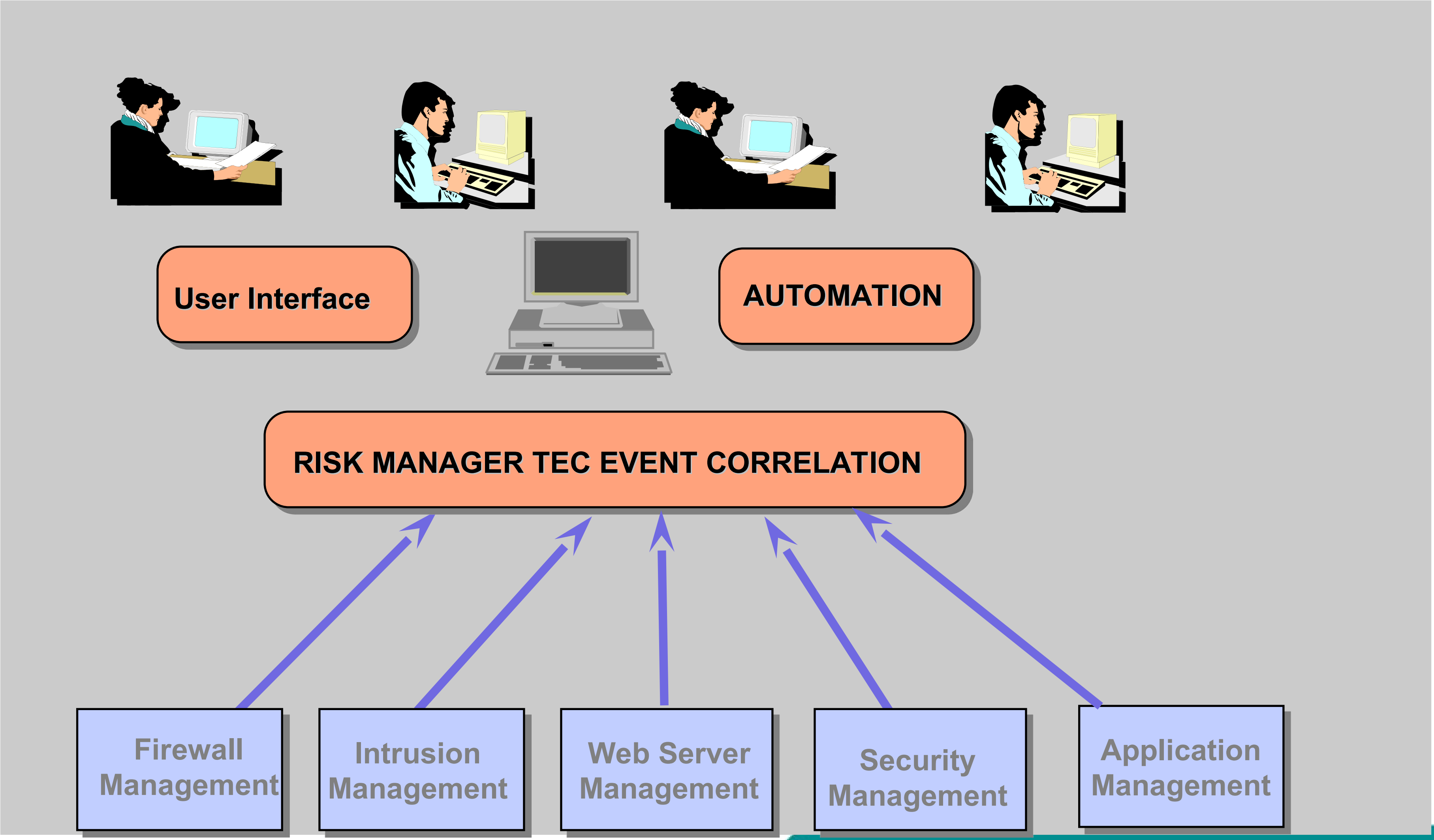
The more we can centrally correlate, the better we can manage the distributed threats & intrusions

Tivoli SecureWay Risk Manager

- Centralized management of enterprise risks (intrusion-detection, firewalls, Web Servers etc)
- Based on IBM Zurich Research work
- Strength is in management & central correlation of security events, reduction of false positives, provisioning of adaptive security
- Benefit: Reduced security risks: Faster detection and assessment of security breaches, and quicker responses

Risk Manager is the Communications and control center for centrally managing e-business vulnerabilities

Risk Manager - Tivoli Enterprise Solution



Tivoli

Risk Manager Features

- Centralized management Correlation of Intrusions
- New realtime Web Intrusion Detection System designed for Web Server attacks
- Support for ISS RealSecure and Cisco Secure IDS
- Leverages Tivoli Management Framework/TEC Console
- Tivoli Plus Modules extend capability for centralized reporting of alerts to TEC

Centralized Correlation

- Manual Correlation across point products is impossible
- Without correlation there are too many false positives
- Administrative nightmare to identify real attacks from false positives
- Present one alarm per attack, even if this attack has generated many intrusion detection events
- Simplify administration for non-security experts

We need a better design, one that collects input from multiple different sensors and intelligently correlates the outputs and alerts from each sensor to determine if there is truly an attack.

Web Intrusion Detection System (Web IDS)

- Realtime Intrusion Detection System for Web Servers
- Required as Network IDSs are limited capability to detect Web attacks
- Specifically designed for content-based attacks on URL using HTTP
- Detects Web attacks launched using HTTP or HTTPS
- Does not detect operating-system attacks or attacks against other services

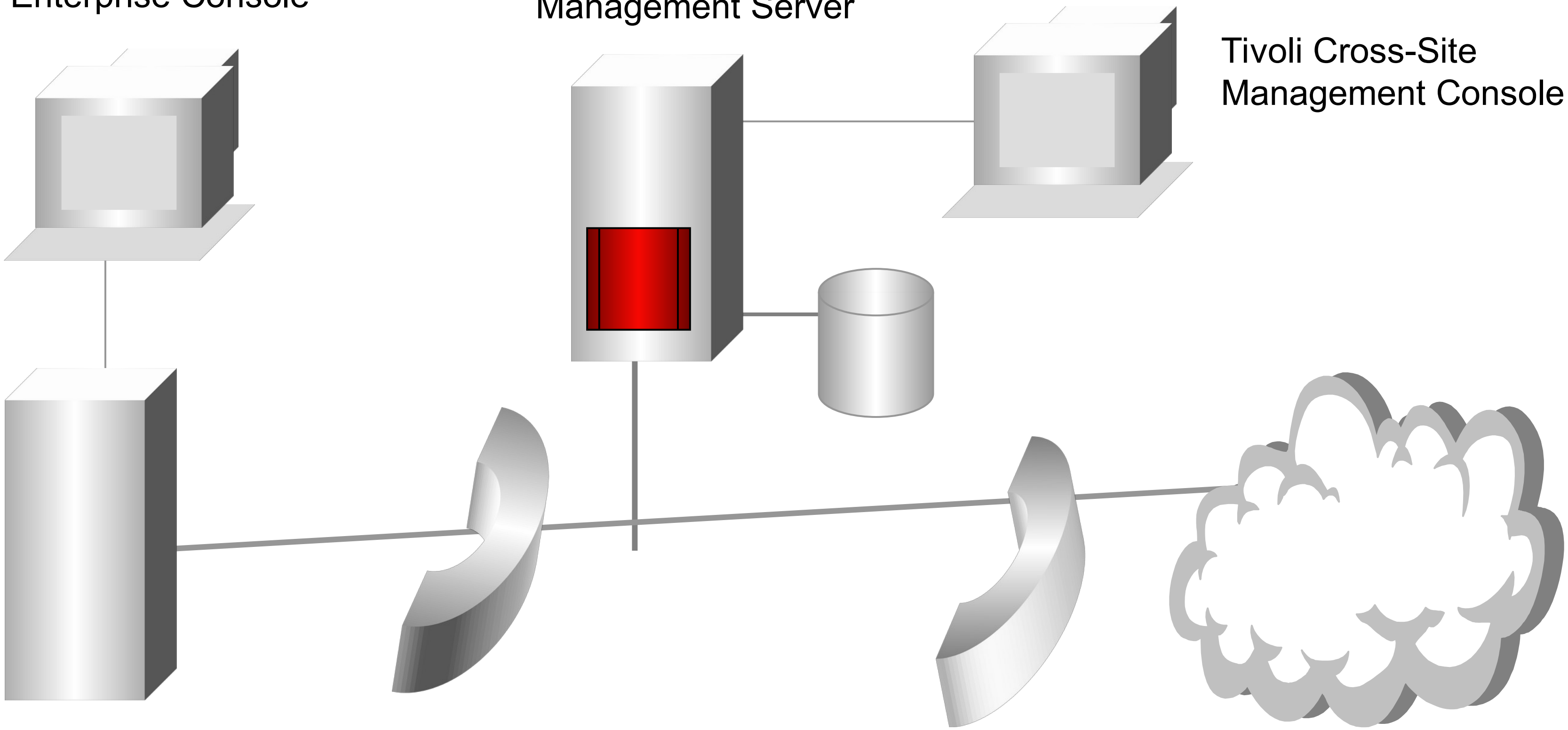
ISS RealSecure Adapter

- Risk Manager Adapter for RealSecure Network IDS
- Version:
  - ISS RealSecure Network IDS version 3.2
- ISS Platform:
  - Windows NT Console
  - RealSecure sensors could be deployed on NT or Solaris
- Centralized correlation across multiple sensor locations using TEC Rules

Cisco Secure IDS

- Risk Manager Adapter for Cisco Secure IDS (formerly NetRanger)
- Version:
  - Cisco NetRanger Network IDS version 2.2
- Platform
  - Solaris 2.7
- Centralized correlation across multiple sensor locations using TEC Rules

Tivoli Cross-Site for Security



Tivoli Enterprise Console

Tivoli Cross-Site Management Server

Tivoli Cross-Site Management Console

Tivoli Enterprise Server

Risk Manager correlates alerts from Cross-Site Security* Intrusion Detection System

*Available in R1 refresh

Risk Manager Leverages Tivoli Framework

- Tivoli Management Framework
- Tivoli Enterprise Console
  - Centralized Intrusion correlation, Management and reporting
- **Tivoli Security Manager**
  - Security Manager supports stringent access control, host violations, and centralized Audit capability for Enterprise servers.
- **Tivoli Policy Director**
  - Policy Director provides granular access control for Web Servers whereas Risk Manager provides intrusion detection and correlation for Web servers protected by Policy Director

Together, these solutions reinforce each other to provide complete protection for the Enterprise

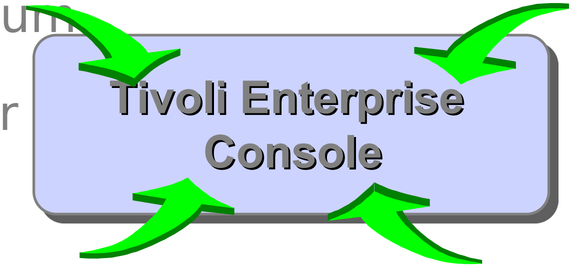
Tivoli / TEC Event Integration

- HP OpenView
- SunNet Manager/Solstice
- Cabletron Spectrum
- Tivoli NetView
- Tivoli NetView for
- Generic SNMP

- Unix
- NT
- AS/400
- OS/2
- Tandem NSK

- Tivoli Distributed Monitoring
- Tivoli Software Distribution
- Tivoli SecureWay Security Manager
- Tivoli Global Enterprise Manager
- and more .....

- All AMS-ready applications



Tivoli Manager For

- Domino
- SAP R3
- MQ Series
- CATIA
- SuiteSpot
- MCIS
- Oracle
- Sybase
- Informix
- MS SQL Server
- DB/2
- and more ......

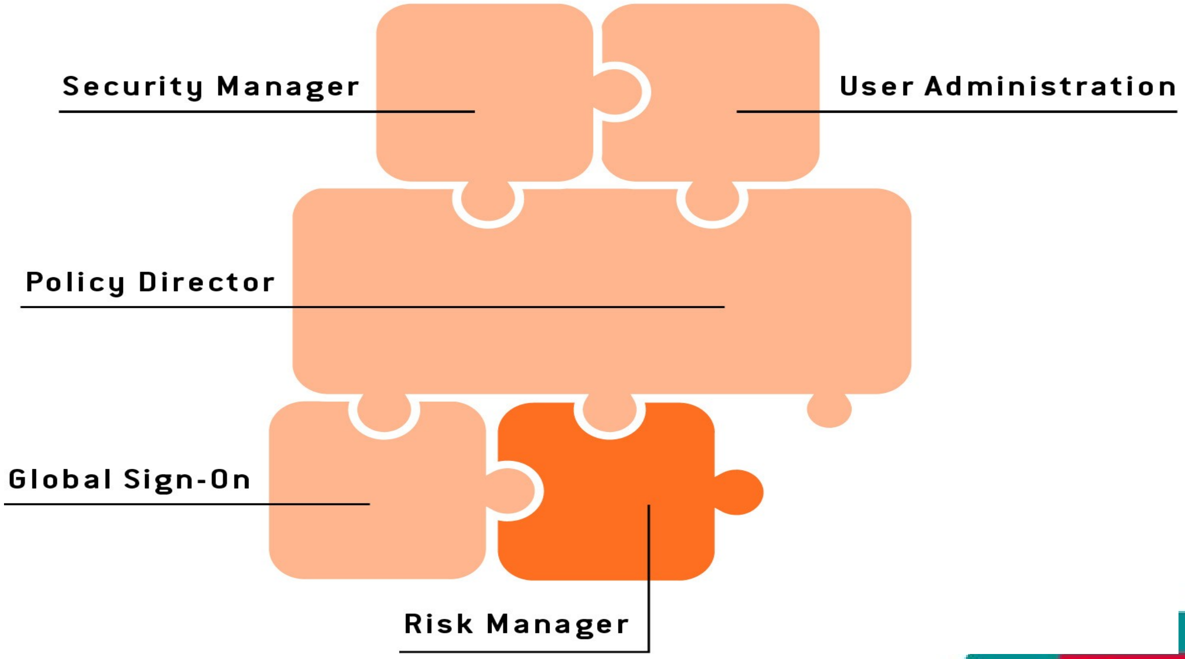
Tivoli PLUS for

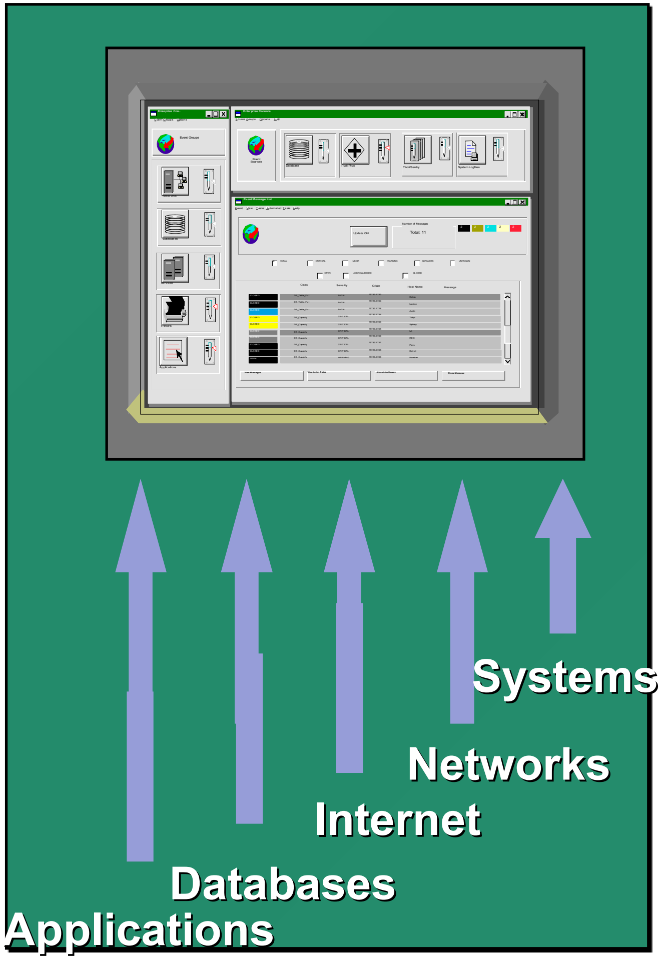
- Remedy ARS
- Maestro
- Legato Networker
- ADSM
- Every certified 10PLUS partner product (growing list !!)

Managing e-business Threats : The Tivoli Solution

- Security Manager for Policy Management
- Policy Director for Web I&A, Access Control
- Distributed Monitoring for Host Monitoring
- TEC for Correlation
- Tivoli Decision Support

Tivoli SecureWay Family —





Tivoli Ready Security Products

- Checkpoint (Firewall-1 and VPN-1)
- Symantec Norton AntiVirus
- Axent (ESM, ITA)
- ISS RealSecure

Tivoli Business Partners

- IBM Global Services
- Ernst &Young
- Deloitte & Touche

Conclusion

- To defend against attacks,intrusions of any kind requires products, policies & management.
- We have abundance of point products. What is missing is an integrated security management capability that correlates intrusion alert information across point solutions
- Tivoli SecureWay Risk Manager is a management solution that enables customers to implement an integrated security management strategy

Tivoli SecureWay - Partnering For Your Success

CHECK POINT™
Software Technologies Ltd.

ERNST & YOUNG
FROM THOUGHT TO FINISH™

RSA
SECURITY

Deloitte & Touche

Entrust®
Technologies

Discover IBM Global Services
People who think. People who do. People who get it.™

ISS
home

Tivoli SecureWay

Tivoli

Manage. Anything. Anywhere.™