Hacker Savvy. Enterprise Smart.

Introducing Defiance™

Intelligent Web Application Security Management

January 2005

Agenda

- **The need for Web applications security**
- **Evaluating the options**
- **Why Defiance TMS?**
- **Defiance TMS**
  - Features & Benefits
  - Pricing & Availability
- **Summary**
- **Kavado Highlights**

Web application security- a known problem

“The most damaging targeted attacks — those against specific businesses — have focused on vulnerabilities in Web applications and custom-developed software." ***--Gartner, July 2004***

"By 2006, Gartner claims, 80 percent of application development teams will have a person or team responsible for application security. "

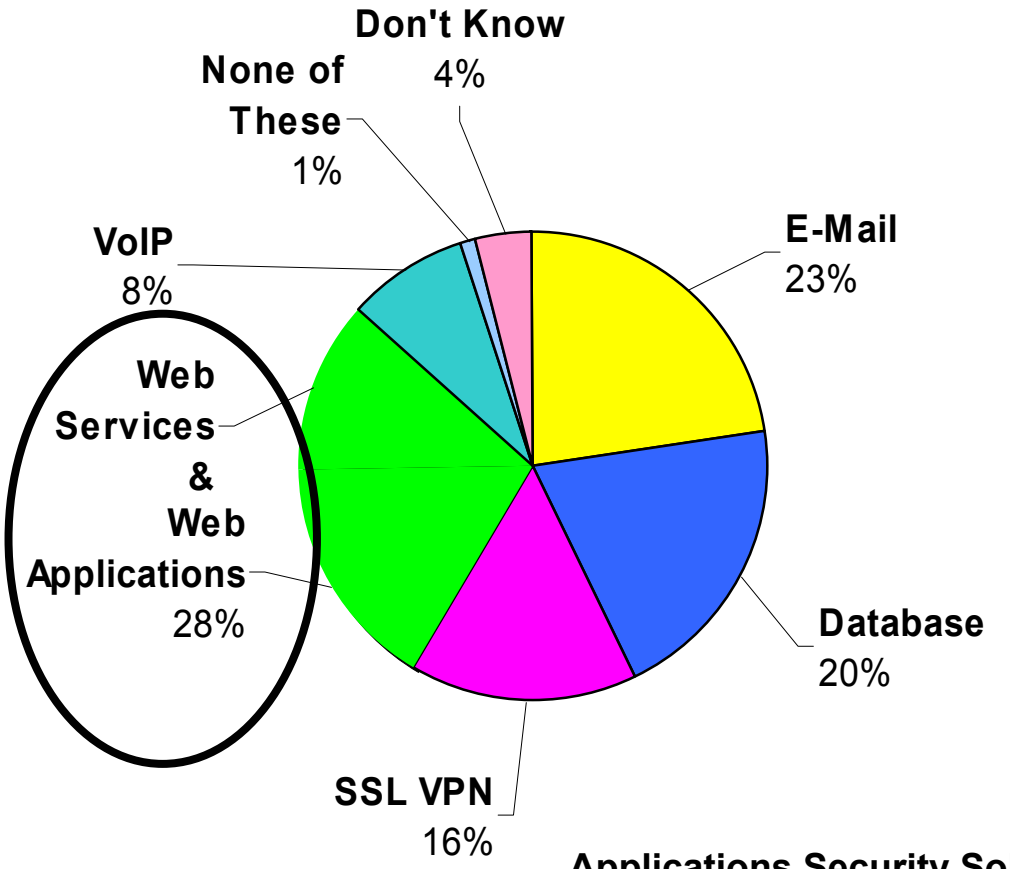
--eWeek, September 2004

“The battle between hackers and security professionals has moved from the network [to the] applications themselves."

-- Network World, May 2004

Enterprise IS Budgets - 2005 Projections

Yankee Group 2004: "Web application security gateways are positioned for growth"



Applications Security Solutions Ranked 1, 2 or 3 in Importance to Respondents' Companies

Source: The Yankee Group 2004 Enterprise Security Spending Survey

Recent Attacks

"Pet retailer Petco Animal Supplies Inc. has agreed to beef up its computer security to settle charges that it left customers' credit-card numbers vulnerable to hackers…"

--Reuters, Nov. 2004

"Hackers took advantage of a known vulnerability on an unpatched computer to potentially gain access to some 1.4 million names, Social Security numbers, telephone numbers, addresses and dates of birth at University of California at Berkeley ."

--eWeek, Oct. 2004

"Guess.com was open to an "SQL injection attack," permitting anyone able to construct a properly-crafted URL to pull down every name, credit card number and expiration date in the site's customer database -- over 200,000 in all…"

-- SecurityFocus, Dec. 2003

"A security loophole at internet bank Cahoot briefly allowed customers to access other people's accounts ..."

--BBC News, Nov. 2004

Increase in attacks to high profile sites show hackers are now targeting the application layer

Threats Now Exist at the Application Layer

Companies in financial services, healthcare, government, and other industries are moving supply chain, CRM, and other critical applications online

However traditional security measures – Network IPS and firewalls – fail to prevent attacks at the application layer

Strong security at the network layer causes hackers to pursue attacks at the vulnerable application layer

This failure leaves sensitive customer data (e.g. credit cards) and corporate assets (e.g. financial information) exposed to business and compliance risk

Kavado's solutions protect enterprises from attacks to their most critical Web-based applications

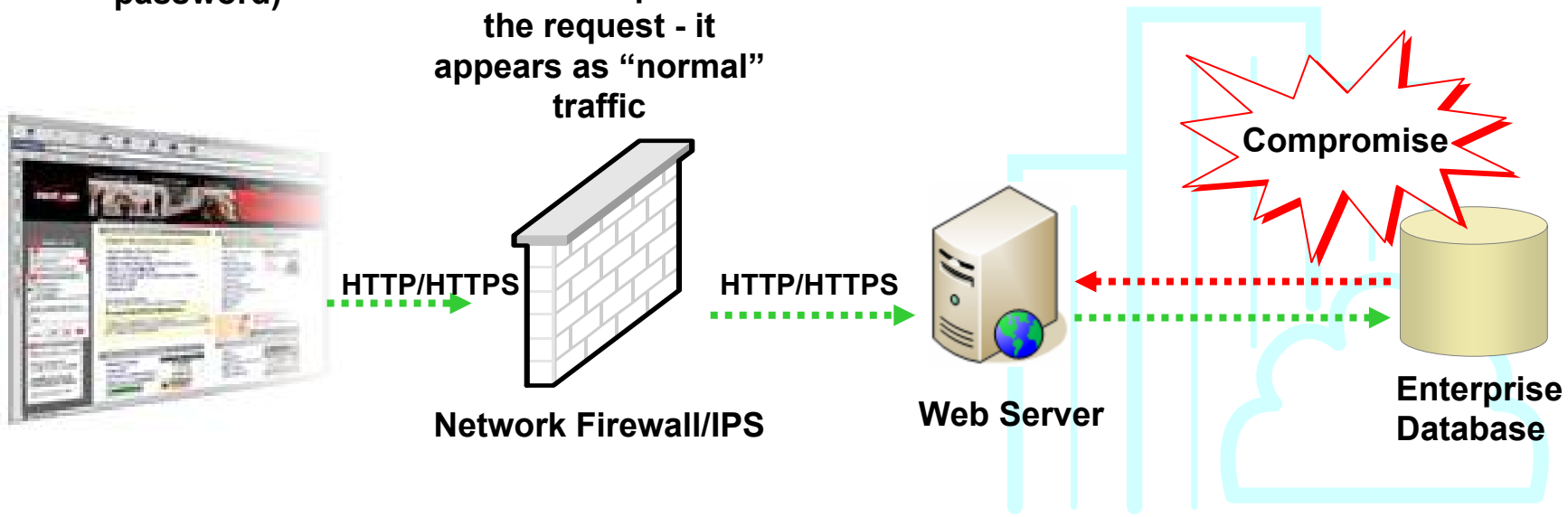
Web Application Attack - SQL injection example

HACKER navigates to a standard form page, but inserts SQL command into a data field (e.g. password)

NETWORK FIREWALL passes the request - it appears as "normal" traffic

WEB SERVER passes the "normal" request AND the **"HACK"** SQL command to the database

DATABASE potentially responds to SQL injection with private customer data or corrupts corporate database



Potential solution #1

Doing nothing leaves critical Web applications vulnerable to attack, and can expose the business to significant regulatory and business risks

Technical Risks:

- Theft of corporate intellectual property
- Identity theft, loss of sensitive customer data
- Destruction of corporate assets
- Critical application downtime

Business Risks:

- Lost sales or customer dissatisfaction
- Regulatory & audit exposure
- Legal liability
- Loss of credibility with consumers and the business
- Increased IT cost

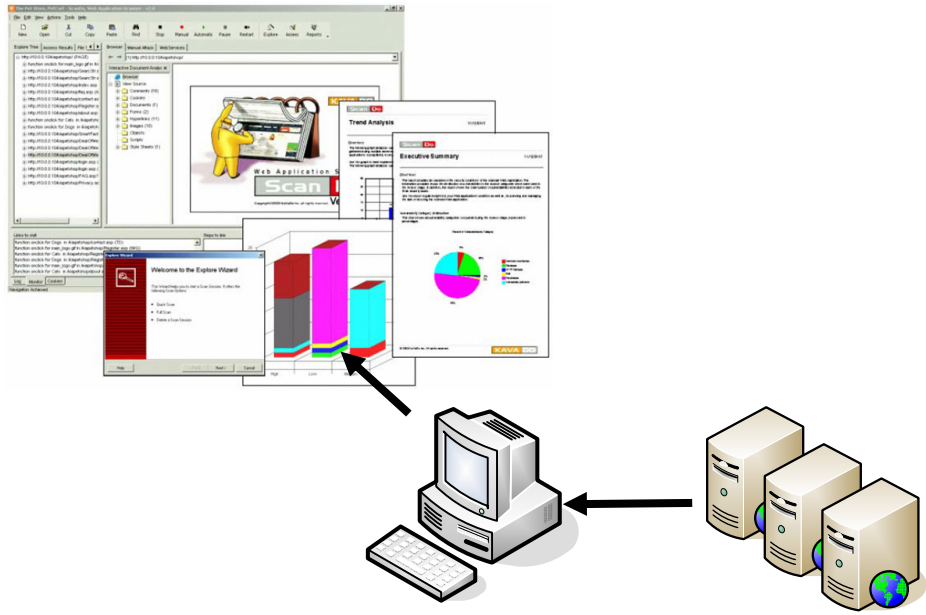
Potential solution # 2

Addressing vulnerabilities in development conforms with best practices and is a less costly solution for new applications during coding

"Removing a security vulnerability during test is < 2% of the cost of removing it from production system" *--John Pescatore, Gartner 2004*

But…

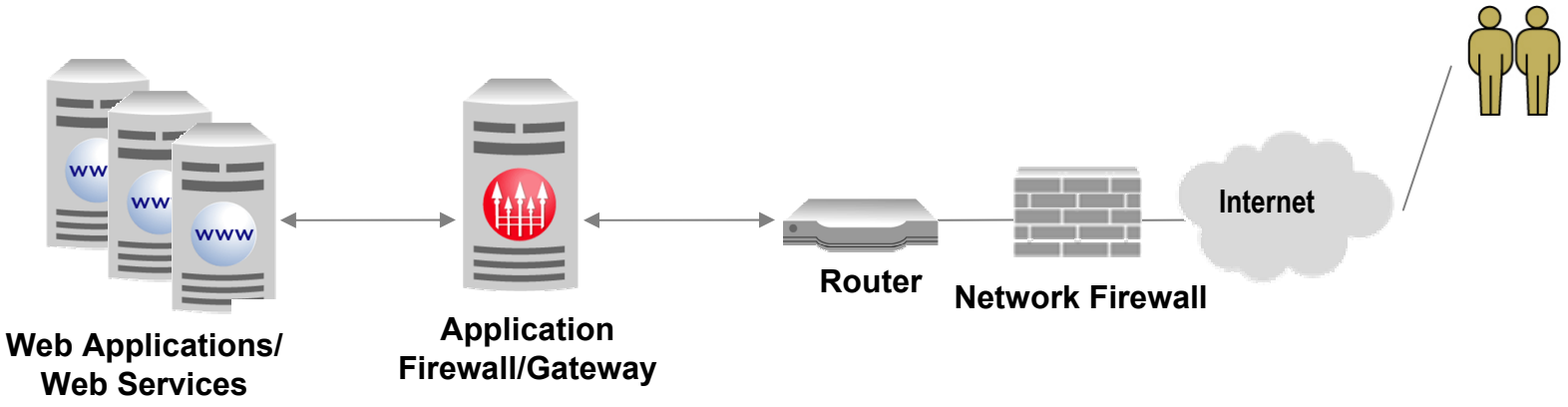
- For applications in production, new threats are continuously emerging
- Vulnerabilities can't always be addressed immediately (resource prioritization)



Potential solution #3

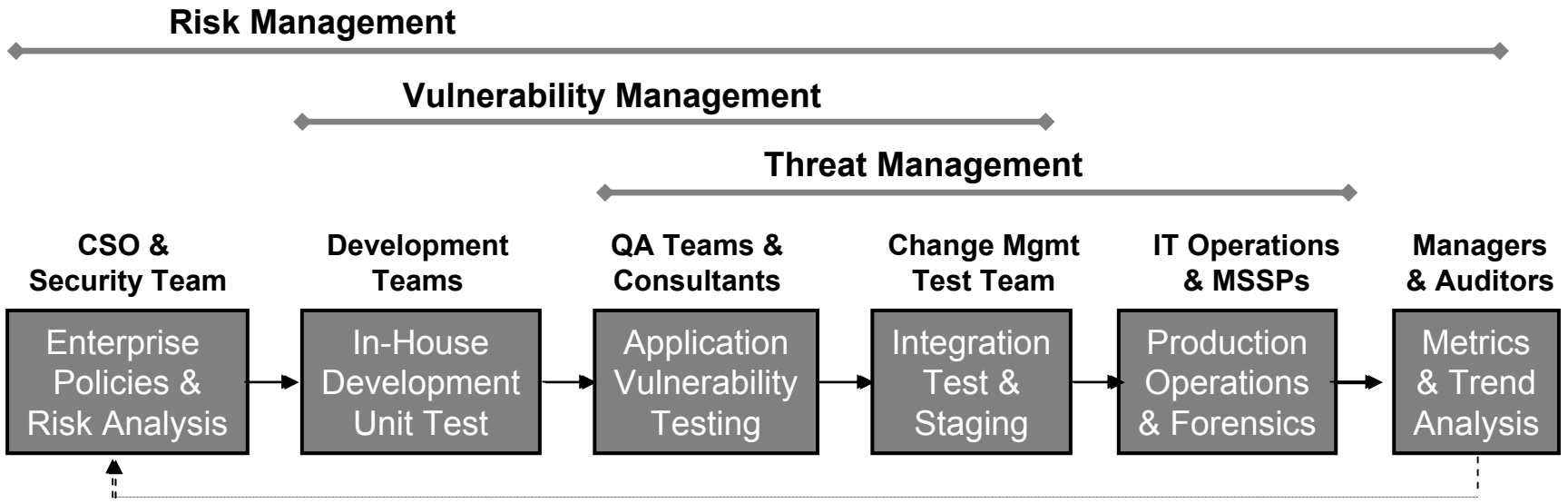
Addressing threats in production protects against known and unknown attacks, with immediate protection for applications in/close to deployment

"Gartner believes it will become increasingly common for attacks to occur less than 30 days after a patch release. Gartner projects that by 2006, such attacks will represent 30 percent of all attacks, up from 15 percent in 2004." *----John Pescatore, Gartner 2004*



Security is a continuous process

Web applications are in a constant state of change, so security isn't a one-time fix. "Where to start" depends on where the application is in the lifecycle.



Case Example #1

Background

Global 500 company is moving its procurement applications online **using a leading CRM solution**, supporting over $1B in transactions

Challenge

Significant vulnerabilities were discovered at the application layer that **could not be fixed quickly in the code.** The company was seeking a security solution that could be deployed in production

Solution

Kavado won the bid after an extensive evaluation versus Checkpoint and Watchfire

Results

Company is now planning to **deploy Defiance TMS** across **over 680 Web servers**, protecting its critical Web applications across the enterprise

Why Defiance TMS?

Adoption of threat management solutions for Web applications security is increasing

- Receiving increasing numbers of RFPs from Global 500 companies for enterprise-wide deployment; several large pilots in progress

- **But current products in the industry are point solutions, and don't meet the needs of large, distributed enterprises**
  - ✓ **Scalability** & centralized management
  - ✓ **Maximum security** without impact to performance
  - ✓ **Visibility** across organizational roles
  - ✓ **Rapid deployment**
  - ✓ **Flexible architecture**

Defiance TMS addresses the needs of Global 500 enterprises deploying large-scale Web applications in a distributed environment

Case example #2

Background

A major multinational operates one of the **largest consumer e-commerce sites** in Asia, supporting tens of thousands of transactions per second

Challenge

Vulnerabilities allowed a primarily young target audience to **steal valuable music** and other media content, resulting in revenue loss

Solution

Kavado won the bid against Teros & Netcontinuum, due to flexibility and ease of use

Results

Company has budgeted over $3M to deploy Defiance TMS as the corporate standard for Web applications in 2005 and beyond, across all subsidiaries

Introducing Defiance™ TMS

Defiance TMS is the first comprehensive Threat Management System to support large-scale deployment of Web applications and Web services security for the distributed enterprise.

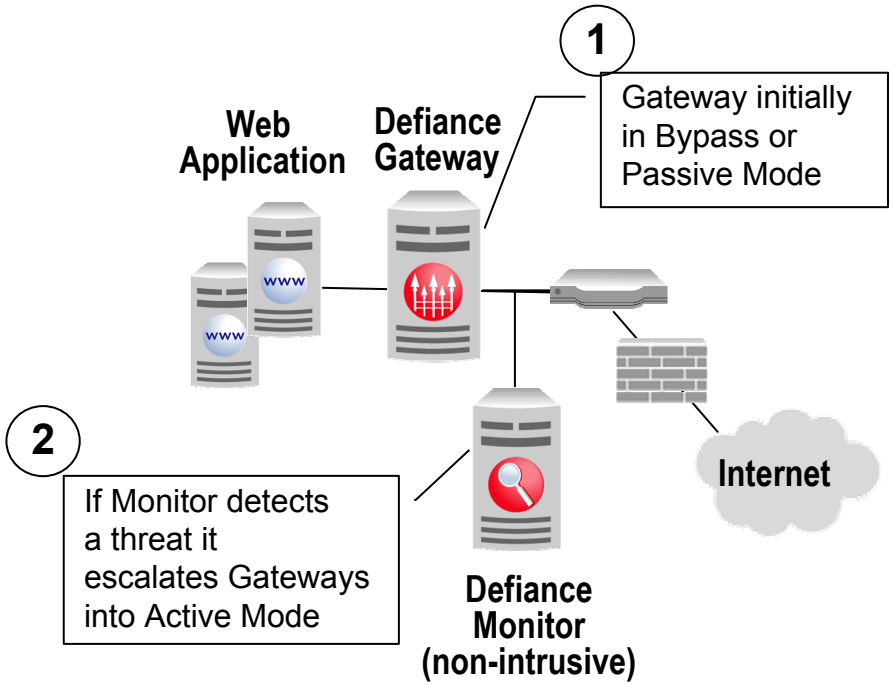
Key Components:

Defiance Monitor	→	Web application Intrusion Detection System
Defiance Gateway	→	Web application Intrusion Prevention System
Defiance Security Console	→	Centralized administration, management, reporting, forensics
Defiance Management Server	→	Consolidated repository of Web application security data and logs

Defiance™ TMS

Patent-pending Intelligent Escalation technology

With Intelligent Escalation™ technology, Defiance Gateways & Monitors work seamlessly to detect threats, generate alerts, and block attacks



Benefits:

Maximizes attack protection

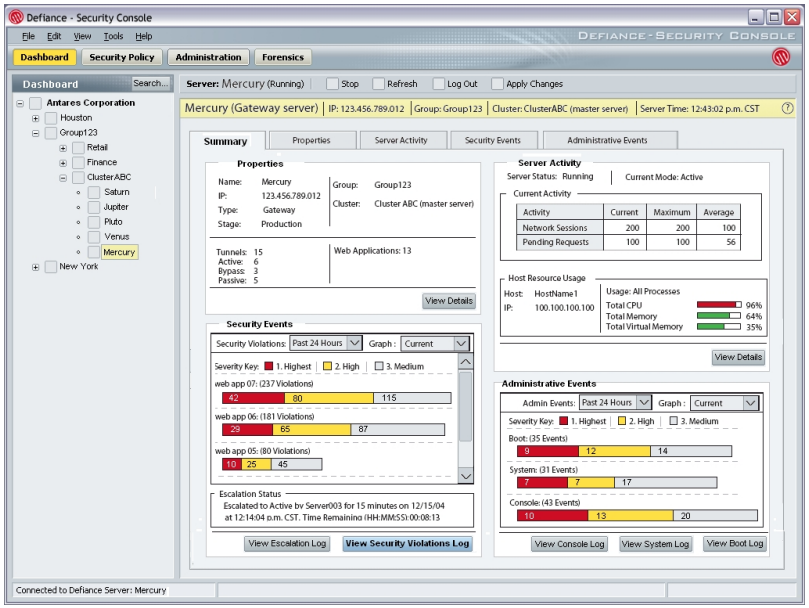
- Threat at a single location results in coordinated response by Defiance Gateways and Monitors across the enterprise

Provides flexibility and control

- Adjust level of security based on business and information risk

Defiance™ TMS
Security Console

Provides centralized administration, management, reporting, and forensics for Monitors and Gateways across the enterprise



Provides 4 views into Security: 1) Administration, 2) Security Policies, 3) Dashboard, 4) Forensics

Benefits:

Enterprise-Class Scalability

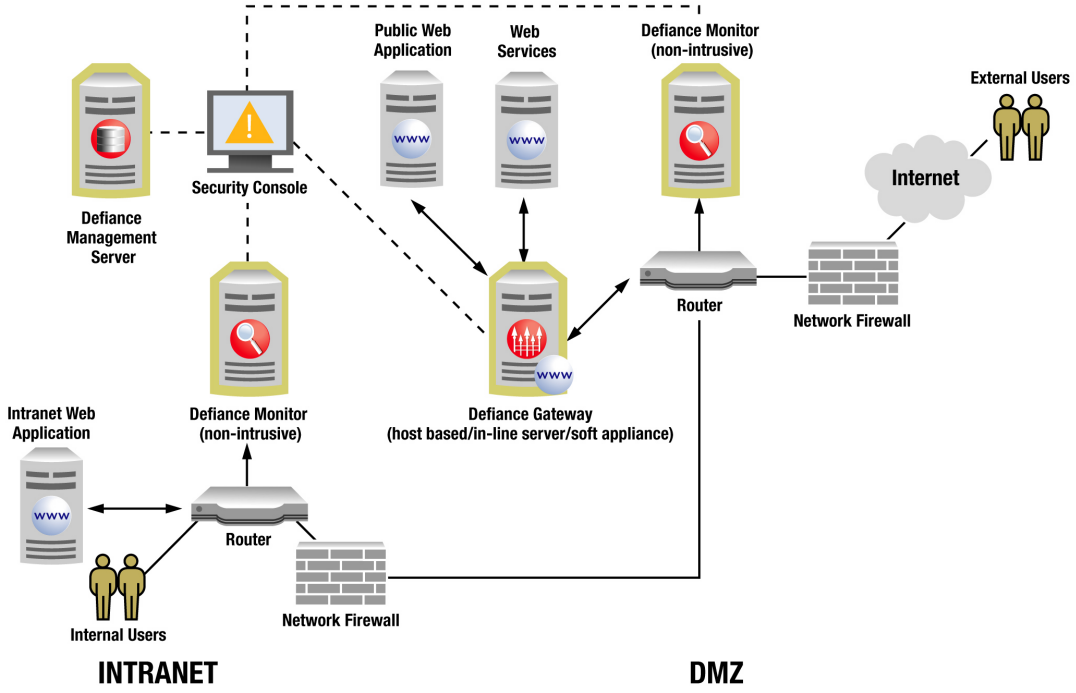
- Centralized management for Defiance Monitors and Gateways enterprise-wide

Visibility Across Organizational Roles

- Supports needs of senior security officers to IT operations, audit, and the business

Defiance™ TMS
Flexible architecture

Defiance TMS architecture is highly flexible, and can be deployed quickly and scalably to secure Intranet, Internet, and Extranet applications



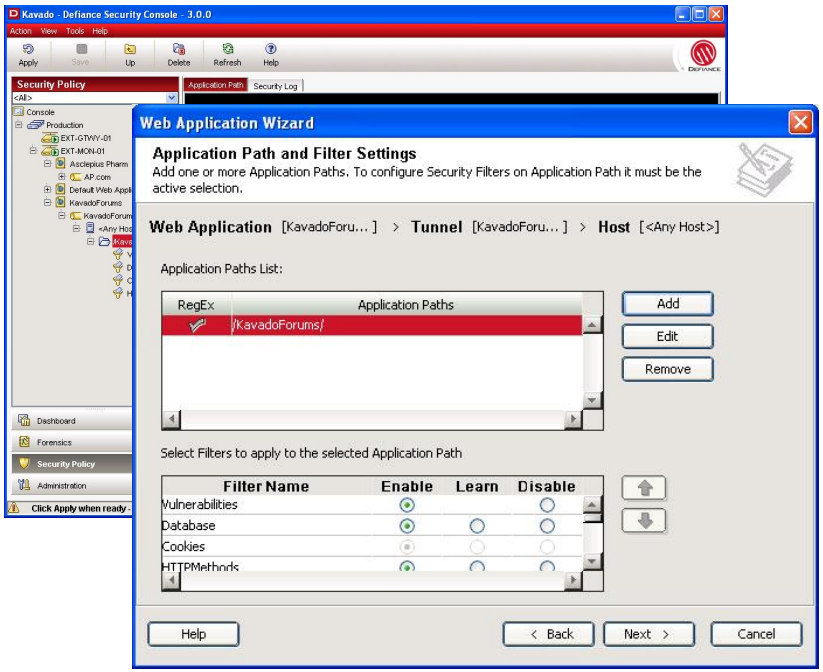
Benefits:

Supports existing IT infrastructure, standards, and procedures

- Linux, Windows or Sun Servers
- Host-based or separate server
- Soft appliance option
- Supports leading EMS (Symantec, IBM Tivoli)
- Supports existing organizational roles

Defiance™ TMS
Policy management

Out-of-the box security policies provide immediate protection, allowing more customized security policies to be established over time



Benefits:

Immediate protection

- Out of the box security policies protect against known & unknown attacks

Easily customizable over time

- Learn mode & quick click refinement
- Refine policies on Defiance Monitor without impact to operations, and quickly replicate to Gateways

Key Points Summary

Enterprises are moving beyond point solutions and are budgeting for large-scale deployment of Web application security in 2005

- **Defiance TMS** is the first solution to provide scalable Web application security for the distributed enterprise
- **Defiance TMS** is the first solution to incorporate coordinated intrusion detection and prevention to detect threats, generate alerts, and block attacks without impacting day-to-day operations
- **Defiance TMS** can be deployed rapidly with existing IT infrastructure and provides maximum threat protection

Kavado Highlights

Company Overview

- **World-class business, technology, and security expertise**
  - **Visionary senior management** with experience from technology leaders Radware, Netegrity, Gartner, Computer Associates, Transcentive, Segue Software, Intel, Yahoo
  - **Leading international investors** – Pequot Ventures, 3i, Platinum Neurone Ventures, Banc of America Equity Partners
  - **Deep technology expertise** – Israel-based R&D
  - **Established 2000,** experienced industry player

- **Strong market position and customer base**
  - 200+ production installations, including 5 of the top 12 Fortune 100
  - Worldwide operations in US, Europe, Middle East and Asia

- **Leading-edge products and technologies**
  - Award-winning **Web application security suite** based on patent-pending technology

Customer Success

KAVADO

Financial Services

HSBC

bank hapoalim

Regions

Goldman Sachs

Paymentech
the payment solutions company

THE Vanguard GROUP

NORWICH UNION

Government

TENNESSEE VALLEY AUTHORITY

The Federal Reserve Board

THE DEPARTMENT OF THE TREASURY 1789

FCC Federal Communications Commission

DEPARTMENT OF JUSTICE

Pharmaceuticals

Boehringer Ingelheim

Aventis

Bristol-Myers Squibb Company

BAYER Bayer

Pfizer

Professional Services

ERNST & YOUNG
Quality In Everything We Do

PRICEWATERHOUSECOOPERS

FORSYTHE
Delivering the business value of IT.℠

Grant Thornton

BearingPoint
Formerly KPMG Consulting, Inc.

Key Partnership Development

Technology Alliance Program

Partnerships with leading technology companies to deliver integrated solutions for our customers

Protected Path™ Program

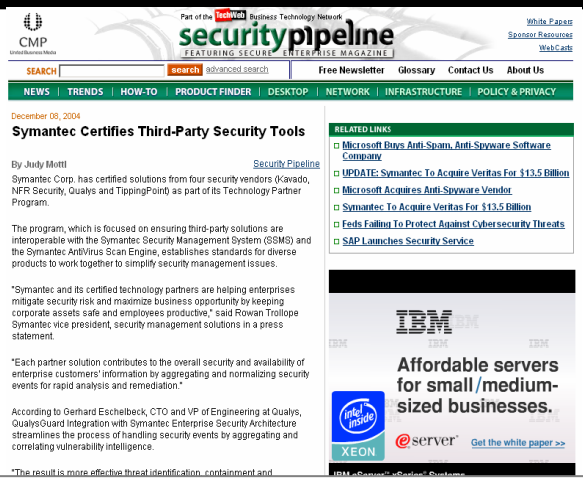
Enables Value Added Resellers, System Integrators, and Service Providers to resell Kavado's Web application security solutions

Consulting Partnerships

Supports security consultants in using Kavado's solutions to help customers meet regulatory and audit requirements

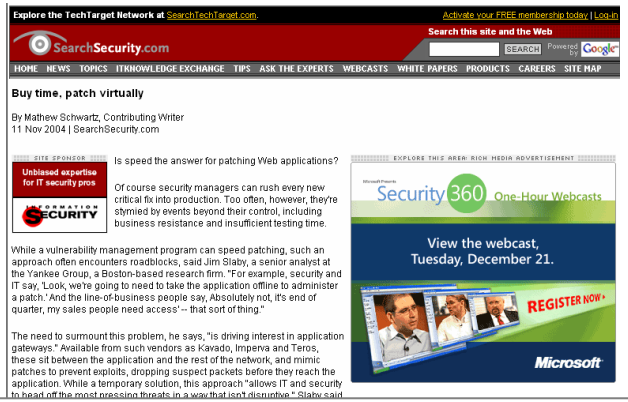
Recent Media Coverage

"Phishing—who's taking the bait now?"
--CNET News.com, Nov 2004



"Symantec Certifies Third-Party Security Tools"
--Security Pipeline, Dec 2004

"Security firms leap in to Cahoot debate"
--InfoSecurity Today, Nov 2004



" Buy time, patch virtually"
--Search Security.com, Nov 2004

Recent Awards for Kavado's solutions

"Kavado customers say ScanDo is a new necessity for organizations that execute critical business processes over the Web. It will typically identify a hole big enough to drive a truck through on the first pass, so payback can often be achieved during the evaluation or pilot period. "

- ***Nina Lytton, president and principal analyst of OSA***

"The 'InfoWorld 100' recognizes companies like Paymentech that made the best use of technology to enhance their businesses. Paymentech built an innovative and proactive Web application security strategy using Kavado's ScanDo to meet critical technical and business objectives."

- ***Steve Fox, editor-in-chief of InfoWorld***

"The Web application protection space is a key space, and Kavado is at the forefront."

- ***Venture Reporter***

"Our annual awards highlight the passing year's key IT trends and unveil our Test Center analysts' picks for the most innovative and effective products in 2004. "

- ***Steve Fox, editor-in-chief of InfoWorld***